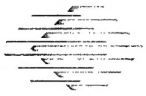


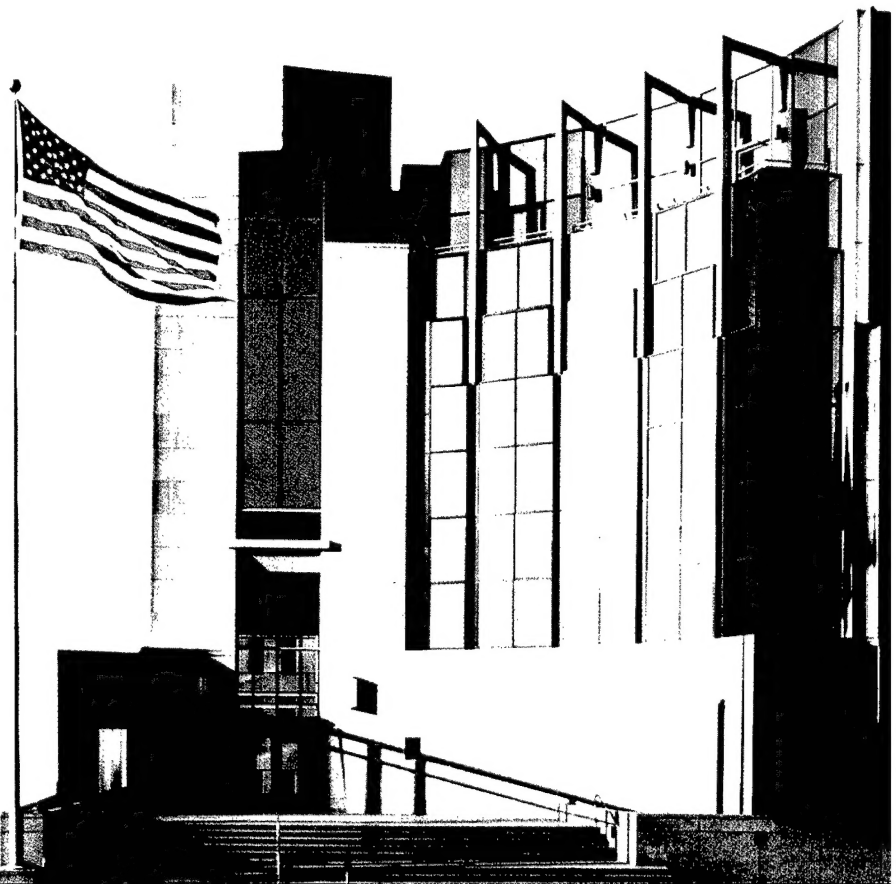
Carnegie Mellon
Software Engineering Institute

OCTAVE®-S Implementation Guide, Version 1.0

Volume 3: Method Guidelines

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005



HANDBOOK
CMU/SEI-2003-HB-003

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

OCTAVE®-S Implementation Guide, Version 1.0

Volume 3: Method Guidelines

CMU/SEI-2003-HB-003

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

Networked Systems Survivability Program

This report was prepared for the

SEI Joint Program Office
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Table of Contents

List of Tables

About This Document

This document is Volume 3 of the *OCTAVE-S Implementation Guide*, a 10-volume handbook supporting the OCTAVE-S methodology. This volume provides the detailed guidelines for conducting an OCTAVE-S evaluation.

The volumes in this handbook are

- *Volume 1: Introduction to OCTAVE-S* – This volume provides a basic description of OCTAVE-S and advice on how to use the guide.
- *Volume 2: Preparation Guidelines* – This volume contains background and guidance for preparing to conduct an OCTAVE-S evaluation.
- ***Volume 3: Method Guidelines*** – This volume includes detailed guidance for each OCTAVE-S activity.
- *Volume 4: Organizational Information Workbook* – This volume provides worksheets for all organizational-level information gathered and analyzed during OCTAVE-S.
- *Volume 5: Critical Asset Workbook for Information* – This volume provides worksheets to document data related to critical assets that are categorized as information.
- *Volume 6: Critical Asset Workbook for Systems* – This volume provides worksheets to document data related to critical assets that are categorized as systems.
- *Volume 7: Critical Asset Workbook for Applications* – This volume provides worksheets to document data related to critical assets that are categorized as applications.
- *Volume 8: Critical Asset Workbook for People* – This volume provides worksheets to document data related to critical assets that are categorized as people.
- *Volume 9: Strategy and Plan Workbook* – This volume provides worksheets to record the current and desired protection strategy and the risk mitigation plans.
- *Volume 10: Example Scenario* – This volume includes a detailed scenario illustrating a completed set of worksheets.

Abstract

The Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE®) approach defines a risk-based strategic assessment and planning technique for security. OCTAVE is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organizations (less than 100 people). OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organization's personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization's unique operational security risks. To conduct OCTAVE-S effectively, the team must have broad knowledge of the organization's business and security processes, so it will be able to conduct all activities by itself.

Introduction

This document contains the Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE®)-S method guidance. This volume provides detailed guidelines and some specific examples for each activity in OCTAVE-S. A complete example showing the key worksheets and results is provided in Volume 10 and can be used as an aid in understanding the method guidance. The worksheets referred to in the guidance are all contained in Volumes 4 through 9 of this handbook.

[SM] Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University.

® OCTAVE is registered in the United States Patent and Trademark Office by Carnegie Mellon University.

Activities Applicable to All Phases and Processes

The following activities can occur during any phase or process of OCTAVE-S:

- Develop action list
- Document notes and recommendations

Develop Action List

Develop Action List	All Phases, All Processes, All Steps

Activity Worksheets	*Reference Worksheets*
• Action List (Vol. 9)	• none

Background/Definitions

Action list – a list of near-term action items identified during OCTAVE-S activities

An action item is something that an organization intends to complete in the near term. Action items generally don't require

- specialized training
- policy changes
- changes to roles and responsibilities

Instructions

During the evaluation, you will likely identify near-term actions that need to be completed. As you identify an action item, document that action on the *Action List Worksheet* (Vol. 9). Include the following information for each action item:

- a description of the action
- responsibility for completing the action
- a date for completing the action
- any management actions that could help facilitate completion of the action

Document Notes and Recommendations

Document Notes and Recommendations	All Phases, All Processes, All Steps

Activity Worksheets	*Reference Worksheets*
• Notes and Recommendations (Vol. 9)	• none

Background/Definitions

Notes – background information that you believe is relevant to record (i.e., information that you might want to refer to during a later activity)

Recommendations – ideas that you want to consider when you create mitigation plans or update your protection strategy during Process 5

Instructions

1. During the evaluation, you will likely think of notes or recommendations that you want to consider at a later time. Document each note or recommendation on the *Notes and Recommendations Worksheet* (Vol. 9).
2. Before you begin each process, review the notes and recommendations to reset context.

Phase 1: Build Asset-Based Threat Profiles

Phase 1 is an evaluation of organizational aspects. During this phase, the analysis team defines impact evaluation criteria that will be used later to evaluate risks. It also identifies important organizational assets and evaluates the current security practice of the organization. The team completes all tasks by itself, collecting additional information only when needed. It then selects three to five critical assets to analyze in depth based on relative importance to the organization. Finally, the team defines security requirements and a threat profile for each critical asset. Table 1 illustrates the processes and activities of Phase 1.

Table 1: Processes and Activities of Phase 1

Phase	Process	Activity
Phase 1: Build Asset-Based Threat Profiles	Process S1: Identify Organizational Information	S1.1 Establish Impact Evaluation Criteria
		S1.2 Identify Organizational Assets
		S1.3 Evaluate Organizational Security Practices
	Process S2: Create Threat Profiles	S2.1 Select Critical Assets
		S2.2 Identify Security Requirements for Critical Assets
		S2.3 Identify Threats to Critical Assets

Process S1: Identify Organizational Information

This process focuses on developing criteria for evaluating the impact of risks for the organization, identifying the organization's assets, and evaluating the organization's security practices.

S1.1 Establish Impact Evaluation Criteria

Activity S1.1: Establish Impact Evaluation Criteria	Phase 1, Process S1, Step 1
Activity Worksheets	*Reference Worksheets*
• Impact Evaluation Criteria (Vol. 4)	• none

Background/Definitions

Impact – the effect of a threat on an organization's mission and business objectives

Impact value – a qualitative measure of a specific risk's impact to the organization (high, medium, or low)

Impact evaluation criteria – a set of qualitative measures against which each risk's effect on an organization's mission and business objectives is evaluated. Impact evaluation criteria define ranges of high, medium, and low impacts for an organization.

Instructions

Step 1

1. Define a qualitative set of measures (impact evaluation criteria) against which you will be able to evaluate a risk's effect on your organization's mission and business objectives. Document your criteria on the *Impact Evaluation Criteria Worksheet* (Vol. 4). At a minimum, consider the following impact areas:
   - reputation/customer confidence
   - life/health of customers
   - fines/legal penalties
   - financial
   - productivity
   - other (e.g. Administrative actions such as audits and downsizing)

   Fill in any blanks in the criteria to make them meaningful to your organization. You can also change the words provided or add additional words as necessary.

   Note: Within each impact area, there is an option entitled "other" to insert a unique set of criteria. There is also an impact area entitled "other" available for new or unique impact areas.
2. Cross out any impact areas that do not apply to your organization on the *Impact Evaluation Criteria Worksheet* (Vol. 4).

S1.2 Identify Organizational Assets

Activity S1.2: Identify Organizational Assets Phase 1, Process S1, Step 2

Activity Worksheets	*Reference Worksheets*
• Asset Identification (Vol. 4)	• none

Background/Definitions

Asset – something of value to the enterprise. Information technology assets are the combination of logical and physical assets and are grouped into specific classes (information, systems, services and applications, people).

Asset categories

- information – documented (paper or electronic) *data or intellectual property* used to meet the mission of an organization
- systems – a combination of information, software, and hardware assets that process and store *information*. Any host, client, or server can be considered a system.
- services and applications – software applications and services (operating systems, database applications, networking software, office applications, custom applications, etc.) that process, store, or transmit *information*
- people – the people in an organization who possess *unique skills, knowledge, and experience* that are difficult to replace

In an *information* security risk evaluation, assets should be linked to information in some way.

Instructions

Step 2

1. The first page of the *Asset Identification Worksheet* (Vol. 4) focuses on systems, information, and services and applications. Consider the following questions:
   - What systems do people in your organization need to perform their jobs?
   - What information do people in your organization need to perform their jobs?
   - What applications and services do people in your organization need to perform their jobs?
   - What other assets are closely related to these assets?

   Identify assets in your organization, and document them on the first page of the worksheet.

   Note: Each row in the worksheet contains assets that are related. In addition, you may record an asset in more than one row.

(continued on next page)

Guidelines

Activity S1.2: Identify Organizational Assets (cont.) Phase 1, Process S1, Step 2

Activity Worksheets	*Reference Worksheets*
• Asset Identification (Vol. 4)	• none

Instructions

Step 2 (cont.)

2. The third page of the *Asset Identification Worksheet* (Vol. 4) focuses on people. Consider the following questions:
   - Which people have a special skill or knowledge that is vital to your organization and would be difficult to replace?
   - What are their special skills or knowledge?
   - Which systems do these people use?
   - Which other assets do these people use (i.e., information, services, or applications)?

   Identify people assets in your organization, and document them on the third page of the worksheet.

   Note: You might find yourself iterating between these pages. Make sure that you are as complete as possible and that you document all *relevant* relationships among assets.

S1.3 Evaluate Organizational Security Practices

Activity S1.3: Evaluate Organizational Security Practices	Phase 1, Process S1, Steps 3-4
Activity Worksheets	*Reference Worksheets*
• Security Practices (Vol. 4)	• none

Background/Definitions

A security practice survey enables an analysis team to evaluate the extent to which security practices are reflected in the way its organization manages security.

Security practices – actions that help initiate, implement, and maintain security within an enterprise

Organizational vulnerabilities – weaknesses in organizational policy or practice that can result in unauthorized actions

Catalog of practices – a collection of good strategic and operational security practices that an organization can use to manage its security

Strategic practices – security practices that focus on organizational issues at the policy level. They include business-related issues as well as issues that require organization-wide plans and participation.

Operational practices – security practices that focus on technology-related issues. They include issues related to how people use, interact with, and protect technology on a day-to-day basis.

Stoplight status – how well an organization is performing in a security practice area. The following colors are assigned to an area based on perceived performance in that area:

- Green – The organization is performing the security practices in the area very well; there is no real need for improvement.
- Yellow – The organization is performing the security practices to some extent; there is room for improvement.
- Red – The organization is not performing the security practices in the area; there is significant room for improvement.

The following security practice areas are evaluated in OCTAVE-S.

Strategic Practice Areas	Operational Practice Areas
1. Security Awareness and Training	7. Physical Access Control
2. Security Strategy	8. Monitoring and Auditing Physical Security
3. Security Management	9. System and Network Management
4. Security Policies and Regulations	10. Monitoring and Auditing IT Security
5. Collaborative Security Management	11. Authentication and Authorization
6. Contingency Planning/Disaster Recovery	12. Vulnerability Management
	13. Encryption
	14. Security Architecture and Design
	15. Incident Management

(continued on next page)

Activity S1.3: Evaluate Organizational Security Practices (cont.)	Phase 1, Process S1, Steps 3-4
Activity Worksheets • Security Practices (Vol. 4)	*Reference Worksheets* • none

Instructions

Step 3a

Review the statements in each security practice area on the *Security Practices Worksheet* (Vol. 4) and answer the following question:

- To what extent is this statement reflected in your organization?

Circle the best response from the following options:

- *Very much* – The statement represents the current practice in the organization.
- *Somewhat* – The statement partially represents the current practice in the organization. Some aspects of the statement do not represent current practice in the organization.
- *Not at all* – The statement does not represent the current practice in the organization at all.

If you do not know whether a statement reflects security practice in your organization, do not circle any of the responses.

Step 3b

As you complete the survey questions, consider the following questions:

- What is your organization currently doing well in this area?
- What is your organization currently not doing well in this area?

The first question focuses on current security practices used by your organization, while the second centers on organizational vulnerabilities present in your organization.

Record examples of security practices and organizational vulnerabilities relevant to each security practice area.

Step 4

After completing Steps 3a and 3b, assign a stoplight status to each security practice area. The stoplight status should reflect how well you believe your organization is performing in each area. Use the following stoplight definitions as a guide:

- *Green* – The organization is performing the security practices in the area very well; there is no real need for improvement.
- *Yellow* – The organization is performing the security practices to some extent; there is room for improvement.
- *Red* – The organization is not performing the security practices in the area; there is significant room for improvement.

(continued on next page)

Activity S1.3: Evaluate Organizational Security Practices (cont.)	Phase 1, Process S1, Steps 3-4
Activity Worksheets	*Reference Worksheets*
• Security Practices (Vol. 4)	• none

Instructions (cont.)

Action Items, Notes, and Recommendations

1. Document all action items you identified during Process S1 on the *Action List Worksheet* (Vol. 9).

   Include the following information for each action item:

   - a description of the action
   - responsibility for completing the action
   - a date for completing the action
   - any management actions that could help facilitate completion of the action

2. Document notes relevant to the activities in Process S1 on the *Notes and Recommendations Worksheet* (Vol. 9).
3. Document all recommendations from Process S1 that you want to consider during Process S5 on the *Notes and Recommendations Worksheet* (Vol. 9).

Process S2: Create Threat Profiles

This process focuses on selecting critical assets from those previously identified, identifying security requirements for those assets, and identifying threats to those critical assets.

S2.1 Select Critical Assets

Activity S2.1: Select Critical Assets	Phase 1, Process S2, Steps 5-9
Activity Worksheets • Critical Asset Selection (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)	*Reference Worksheets* • Asset Identification (Vol. 4)

Background/Definitions

Critical assets – the most important assets to an organization. The organization will suffer a large adverse impact if

- a critical asset is disclosed to unauthorized people
- a critical asset is modified without authorization
- a critical asset is lost or destroyed
- access to a critical asset is interrupted

Instructions

Note: Before you begin Process S2, review any notes and recommendations that you recorded on the *Notes and Recommendations Worksheets* (Vol. 4) during Process S1. These notes and recommendations could be relevant to the activities that you will conduct during Process S2.

Step 5

Review the assets that you recorded on the *Asset Identification Worksheet* (Vol. 4) and consider the following questions:

- Which assets would have a large adverse impact on the organization if one or more of the following occurred:
  - The asset or assets were disclosed to unauthorized people.
  - The asset or assets were modified without authorization.
  - The asset or assets were lost or destroyed.
  - Access to the asset or assets was interrupted.

As you consider the questions, think about the few information-related assets that are most essential to meeting the organization's mission or achieving its goals and objectives.

Record up to five critical assets on the *Critical Asset Selection Worksheet* (Vol. 4). Also record any relevant notes about each asset.

Note: Completing the "Notes" column is optional. Also, the numbers on the worksheet are not meant to indicate priority order.

(continued on next page)

Activity S2.1 Select Critical Assets (cont.) Phase 1, Process S2, Steps 5-9

Activity Worksheets	*Reference Worksheets*
• Critical Asset Selection (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)	• Asset Identification (Vol. 4)

Instructions (cont.)

Step 6

Start a *Critical Asset Workbook* (Vol. 5-8) for each critical asset.

Note: Each category of critical asset (systems, information, applications, people) has a unique Critical Asset Workbook (Vol. 5-8). The contents are similar for each Critical Asset Workbook, but the questions are worded slightly differently depending on asset category. Make sure that you select the appropriate volume for each critical asset.

Record the name of each critical asset on its *Critical Asset Information Worksheet* located in the appropriate Critical Asset Workbook (Vol. 5-8).

Step 7

Document your rationale for selecting each critical asset on that asset's *Critical Asset Information Worksheet* (Vol. 5-8).

Consider the following question:

- Why is this asset critical to the organization?

Step 8

Record a description for each critical asset on that asset's *Critical Asset Information Worksheet* (Vol. 5-8).

Consider the following questions:

- Who uses the asset?
- Who is responsible for the asset?

Step 9

Record assets that are related to each critical asset on that asset's *Critical Asset Information Worksheet* (Vol. 5-8). Refer to the *Asset Identification Worksheet* (Vol. 4) to determine which assets are related to each critical asset.

Consider the following question:

- Which assets are related to this asset?

S2.2 Identify Security Requirements for Critical Assets

Activity S2.2: Identify Security Requirements for Critical Assets	Phase 1, Process S2, Steps 10-11
Activity Worksheets • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)	*Reference Worksheets* • none

Background/Definitions

Security requirements – statements describing the qualities of information-related assets that are important to an organization. Typical security requirements are confidentiality, integrity, and availability.

Confidentiality – the need to keep proprietary, sensitive, or personal information private and inaccessible to anyone who is not authorized to see it

Integrity – the authenticity, accuracy, and completeness of an asset

Availability – when or how often an asset must be present or ready for use

Note: Security requirements within OCTAVE-S focus on what the requirements should be for an asset, not what they currently are.

Instructions

Step 10

1. Record the security requirements for each critical asset on that asset's *Critical Asset Information Worksheet* (Vol. 5-8).

   Note: Security requirements focus on what the requirements *should* be for an asset, not what they currently are.

   Consider the following question:

   - What are the security requirements for this asset?

   A statement for each category of security requirements is presented on the *Critical Asset Information Worksheet* (Vol. 5-8). If a category is applicable for a critical asset, mark an 'X' in the box next to that category.

2. Complete the security requirement for each applicable category for a critical asset. At a minimum, fill in the blanks provided.

   You can change the words provided or add additional words as necessary.

   Note: A category entitled "other" is provided for additional security requirements that do not fall into the categories of confidentiality, integrity, and availability.

Step 11

For each critical asset, record the most important security requirement on that asset's *Critical Asset Information Worksheet* (Vol. 5-8) by marking an 'X' in the box next to the category of security requirements that is most important for that asset.

Consider the following question:

- Which security requirement is most important for this asset?

S2.3 Identify Threats to Critical Assets

Activity S2.3: Identify Threats to Critical Assets	Phase 1, Process S2, Steps 12-16
Activity Worksheets • Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	*Reference Worksheets* • Threat Translation Guide in appropriate Critical Asset Workbook (Vol. 5-8)

Background/Definitions

Threat – an indication of a potential undesirable event. A threat refers to a situation in which a person could do something undesirable (an attacker initiating a denial-of-service attack against an organization's email server) or a natural occurrence could cause an undesirable outcome (a fire damaging an organization's information technology hardware).

Threat profile – a structured way of presenting a range of threats to a critical asset. Threats in the profile are grouped according to the source of the threat.

Generic threat profile – a catalog of threats that contains a range of all potential threats under consideration. The generic threat profile is a starting point for creating a unique threat profile for each critical asset.

Threats are represented using the following properties:

- Asset – something of value to the enterprise
- Access – how the asset is accessed by an actor (network access, physical access). Access applies only to human actors.
- Actor – who or what may violate the security requirements (confidentiality, integrity, availability) of an asset
- Motive – the intent of an actor (e.g., deliberate or accidental). Motive applies only to human actors.
- Outcome – the immediate result (disclosure, modification, destruction, loss, interruption) of violating the security requirements of an asset

In OCTAVE-S, threats are represented visually in a tree structure, often referred to as a threat tree. There is one threat tree for each of the following categories of threat source:

Category	Definition
Human actors using network access	The threats in this category are network-based threats to an organization's critical assets. They require direct action by a person and can be deliberate or accidental in nature.
Human actors using physical access	The threats in this category are physical threats to an organization's critical assets. They require direct action by a person and can be deliberate or accidental in nature.
System problems	The threats in this category are problems with an organization's information technology systems. Examples include hardware defects, software defects, malicious code (e.g., viruses), and other system-related problems.
Other problems	The threats in this category are problems or situations that are outside the control of an organization. This category of threats includes natural disasters (e.g., floods, earthquakes) and interdependency risks. Interdependency risks include the unavailability of critical infrastructures (e.g., power supply).

(continued on next page)

Activity S2.3: Identify Threats to Critical Assets (cont.) Phase 1, Process S2, Steps 12-16

Activity Worksheets	*Reference Worksheets*
• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	• Threat Translation Guide in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions

Note: Each category of critical asset (systems, information, applications, people) has a unique *Risk Profile Worksheet*. You will find it in the Critical Asset Workbook (Vol. 5-8) for that asset category.

Note: You will complete only selected parts of the *Risk Profile Worksheet* (Steps 12-16) during this activity. You will complete the remaining parts (Steps 22, 24, 26, and 27) later in the evaluation.

Step 12

Note: If you have difficulty interpreting a threat on any threat tree, review the description and examples of that threat in the *Threat Translation Guide* (Vol. 5-8).

1. Select the appropriate worksheet for each critical asset.

   Note: The following four trees apply to systems, information, and services and applications:

   - human actors using network access
   - human actors using physical access
   - system problems
   - other problems

   Note: Only one tree applies to people: other problems.

2. Complete all appropriate threat trees for each critical asset. When marking a threat tree, consider the following questions:

   - For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.
   - For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

   Note: Make sure to mark a threat if there is even a remote possibility that a threat could occur. You will have the opportunity to accept the threat later in the evaluation. Right now, you should look at the widest range of possible threats.

(continued on next page)

Activity S2.3: Identify Threats to Critical Assets (cont.)	Phase 1, Process S2, Steps 12-16
Activity Worksheets • Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	*Reference Worksheets* • Threat Translation Guide in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 13

Note: You complete this step only for the following categories of threat:

- human actors using network access
- human actors using physical access

In this step, you provide additional details about the following actor-motive combinations:

- insiders acting accidentally
- insiders acting deliberately
- outsiders acting accidentally
- outsiders acting deliberately

1. As you complete threat trees for human actors using network access, consider the following question:

   - Which actors pose the biggest threats to this asset via the network?

   Record specific examples of threat actors on the *Risk Profile Worksheet* (Vol. 5-8) for each applicable actor-motive combination.

2. As you complete threat trees for human actors using physical access, consider the following question:

   - Which actors pose the biggest threats to this asset via physical means?

   Record specific examples of threat actors on the *Risk Profile Worksheet* (Vol. 5-8) for each applicable actor-motive combination.

(continued on next page)

Activity S2.3: Identify Threats to Critical Assets (cont.)	Phase 1, Process S2, Steps 12-16
Activity Worksheets • Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	*Reference Worksheets* • Threat Translation Guide in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 14

Note: You complete this step only for the following categories of threat:

- human actors using network access
- human actors using physical access

In this step, you provide additional details about the following actor-motive combinations:

- insiders acting deliberately
- outsiders acting deliberately

1. Consider the following question for both actor-motive combinations:
   - How strong is the actor's motive?

   You are estimating highest motive strength based on the specific actors you identified during Step 13.

   Mark an 'X' in the box next to the best response from the following options:

   - *High* – The actor is focused on attacking your organization, has very defined goals, is specifically targeting the critical asset, will apply extraordinary means to attack the critical asset, and will go to extraordinary lengths to ensure success.
   - *Medium*– The actor is focused on attacking your organization, has general goals, is targeting a range of assets in your organization, has limits on the means that will be applied to attack the critical asset, and has an explicit or implicit exit strategy defining when to abandon the attack.
   - *Low*– The actor is focused on attacking an organization (not necessarily yours), does not have specific goals, is targeting any asset that can be attacked easily, will apply limited means to the attack, and will quickly abandon the attack if success doesn't prove to be easy.

(continued on next page)

Activity S2.3: Identify Threats to Critical Assets (cont.)	Phase 1, Process S2, Steps 12-16
Activity Worksheets • Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	*Reference Worksheets* • Threat Translation Guide in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 14 (cont.)

2. Consider the following question for each estimate of motive strength:
   - How confident are you in this estimate?

   Mark an 'X' in the box next to the best response from the following options:
   - *Very* – You have a considerable amount of objective data related to your estimate. Any reasonable person reviewing the objective data would reach the same conclusion.
   - *Somewhat* – You have a limited amount of objective data related to your estimate. A reasonable person would need to make key inferences and assumptions to reach the same conclusion. However it is likely that a reasonable person would arrive at the same conclusion.
   - *Not at all* – You have little or no objective data related to your estimate. A reasonable person could arrive at a different conclusion because there are little or no objective data upon which to base the estimate.

Step 15

Note: Complete this step for all categories of threat.

1. Consider the following question for each active threat:
   - How often has this threat occurred in the past?

   Review any objective data that you might have (e.g., logs, incident data) as well as subjective data (what people on the analysis team or people in your organization recall). Fill in the blanks in the following statement for each threat:
   - _____ times in _____ years

(continued on next page)

Activity S2.3: Identify Threats to Critical Assets (cont.)	Phase 1, Process S2, Steps 12-16
Activity Worksheets • Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	*Reference Worksheets* • Threat Translation Guide in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 15 (cont.)

2. Consider the following question for each estimate of threat history:
   - How accurate are the data?

   Mark an 'X' in the box next to the best response from the following options:
   - *Very* – You have a considerable amount of objective data related to your estimate. Any reasonable person reviewing the objective data would reach the same conclusion.
   - *Somewhat* – You have a limited amount of objective data related to your estimate. A reasonable person would need to make key inferences and assumptions to reach the same conclusion. However it is likely that a reasonable person would arrive at the same conclusion.
   - *Not at all* – You have little or no objective data related to your estimate. A reasonable person could arrive at a different conclusion because there are little or no objective data upon which to base the estimate.

Step 16

This step provides additional context where appropriate. Give examples, or scenarios, of how specific threats could affect the critical asset. Record additional context and areas of concern for each source of threat.

Action Items, Notes, and Recommendations

1. Document all action items that you identified during Process S2 on the *Action List Worksheet* (Vol. 9).

   Include the following information for each action item:
   - a description of the action
   - responsibility for completing the action
   - a date for completing the action
   - any management actions that could help facilitate completion of the action
2. Document notes relevant to the activities in Process S2 on the *Notes and Recommendations Worksheet* (Vol. 9).
3. Document all recommendations from Process S2 that you want to consider during Process S5 on the *Notes and Recommendations Worksheet* (Vol. 9).

Phase 2: Identify Infrastructure Vulnerabilities

During this phase, the analysis team conducts a high-level review of the organization's computing infrastructure, focusing on the extent to which security is considered by maintainers of the infrastructure. The analysis team first analyzes how people use the computing infrastructure to access critical assets, yielding key classes of components as well as who is responsible for configuring and maintaining those components.

The team then examines the extent to which each responsible party includes security in its information technology practices and processes. The processes and activities of Phase 2 are shown in Table 2.

Table 2: Processes and Activities of Phase 2

Phase	Process	Activity
Phase 2: Identify Infrastructure Vulnerabilities	Process S3: Examine Computing Infrastructure in Relation to Critical Assets	S3.1 Examine Access Paths
		S3.2 Analyze Technology-Related Processes

Process S3: Examine the Computing Infrastructure in Relation to Critical Assets

This process focuses on examining access paths in the infrastructure for the critical assets and then analyzing the technology-related processes associated with the infrastructure.

S3.1 Examine Access Paths

Activity S3.1: Examine Access Paths	Phase 2, Process S3, Steps 17-18
Activity Worksheets • Network Access Paths in appropriate Critical Asset Workbook (Vol. 5-8)	*Reference Worksheets* • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Background/Definitions

Network access paths – ways in which systems, devices, information, or services can be accessed via an organization's network

System of interest – the system or systems that are most closely linked to a critical asset, for example:

- the system where the asset "lives"
- the system where you would go to get an "official" copy of the asset
- the system that gives legitimate users access to a critical asset
- the system that gives a threat actor access to a critical asset

Key classes of components – categories of devices and networks used to access a system of interest. These devices and networks are either part of or related to a system of interest. When legitimate users access a critical asset, they access components from these classes. Threat actors also access components from these classes when the actors deliberately target a critical asset.

Access points – interfaces that directly or indirectly allow access to a system of interest. These interfaces are grouped according to the following categories:

- components of the system of interest
- system access by people
- intermediate access points
- other interfaces and data storage locations
- other systems

System access by people – types of components that people (e.g., users, attackers) use to access a system of interest. These components constitute access points that can originate internally or externally to an organization's systems and networks.

Intermediate access points – networks used to transmit information and applications from the system of interest to people

Data storage locations – additional types of components used to store critical information or provide data support services related to a system of interest (e.g., storage devices used to back up information stored on a system of interest)

Other systems and components – systems that access critical information or services from a system of interest; also, other classes of components that can be used to access critical information or applications from the system of interest

(continued on next page)

Activity S3.1: Examine Access Paths (cont.) Phase 2, Process S3, Steps 17-18

Activity Worksheets	*Reference Worksheets*
• Network Access Paths in appropriate Critical Asset Workbook (Vol. 5-8)	• Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Background/Definitions (cont.)

The standard classes of components considered in OCTAVE-S are described in the table below:

Component Class	Description
Servers	hosts within your information technology infrastructure that provide information technology services to your organization
Internal networks	interconnectivity that links computers and systems. Internal networks are maintained by people within your organization
On-site workstations	hosts on your networks that staff members use to conduct business
Laptops	portable PCs that staff members use to access information remotely via your organization's networks
PDA/wireless components	Devices (such as PDAs, cell phones, and wireless access points) that staff members may use to access information (e.g., email)
Other systems	systems, processes, and/or applications that access critical information or services from a system of interest. Items in this category link to or use content from the system of interest in some manner.
Storage devices	devices where information is stored, often for backup purposes
External networks	interconnectivity that links computers and systems. External networks are not part of your organization's networks (e.g., the Internet) or are managed for your organization by an external organization.
Home/external workstations	devices that staff members and individuals outside of your organization use to access information remotely via your organization's networks
Others	any other type of device that could be part of your threat scenarios, but does not fall into the above classes

(continued on next page)

Activity S3.1: Examine Access Paths (cont.) Phase 2, Process S3, Steps 17-18

Activity Worksheets	*Reference Worksheets*
• Network Access Paths in appropriate Critical Asset Workbook (Vol. 5-8)	• Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions

Note: Before you begin Process S3, review any notes and recommendations that you recorded on the *Notes and Recommendations Worksheet* (Vol. 9) during previous processes. These notes and recommendations could be relevant to the activities that you will conduct during Process S3.

Complete the steps in this activity for each critical asset that is subject to network-based threats.

OCTAVE-S requires you to perform a cursory examination of how you access critical assets via your organization's networks as well as the extent to which security is considered when configuring and maintaining your organization's computers and networks. If you find that your analysis team is unable to perform Activity S3.1, the members of the team might not possess the necessary skills for the activity and you may need to augment the team's skill set for Activity S3.1. If you do not have anyone within your organization with the appropriate skills for the activity, record a note indicating that the organization lacks people with a basic understanding of computer networking on the *Notes and Recommendations Worksheet* (Vol. 9). If appropriate, you can also record a recommendation for addressing the situation.

Step 17

First, you need to establish the system(s) that is most closely linked to a critical asset. You should think about where the asset "lives," where you would go to get an "official" copy of the asset, the system that gives legitimate users access to a critical asset, and the systems that a threat actor would target to access a critical asset.

Consider the following question:

- Which system or systems are most closely linked to the critical asset? On which system(s) is the critical asset stored and processed?

You could identify multiple systems of interest for a critical asset. Try to narrow the list to the "official" source for the asset.

Record the name(s) of the system(s) of interest on the *Network Access Paths Worksheet* (Vol. 5-8).

Note: If you are analyzing a systems asset, the system of interest is the system itself.

(continued on next page)

Activity S3.1: Examine Access Paths (cont.) Phase 2, Process S3, Steps 17-18

Activity Worksheets	*Reference Worksheets*
• Network Access Paths in appropriate Critical Asset Workbook (Vol. 5-8)	• Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 18a

1. When you examine access paths, you first establish which components are part of the system of interest. Consider the following question:

   - Which of the following classes of components is part of the system of interest?

   After considering the question, mark an 'X' in each box next to each appropriate response in the "System of Interest" area on the *Network Access Paths Worksheet* (Vol. 5-8). You are presented with the following options:

   - servers
   - internal networks
   - on-site workstations
   - others

   If you select "others," be sure to list specific classes of components.

2. When you select a key class of components, document any relevant subclasses or cite specific examples when appropriate. For example, if you select "on-site workstations," you might find it necessary to further refine the designation based on classes of users. Thus, if workstations are configured differently based on how they are used, you could determine that "on-site workstations" includes two subclasses of workstations: staff and management.

(continued on next page)

Activity S3.1: Examine Access Paths (cont.) Phase 2, Process S3, Steps 17-18

Activity Worksheets	*Reference Worksheets*
• Network Access Paths in appropriate Critical Asset Workbook (Vol. 5-8)	• Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 18b

1. Determine how information and applications from the system of interest is transmitted to people who access that system. Consider the following question:
   - Which types of components are used to transmit information and applications from the system of interest to people?

   Note: You might decide that you need to first review the types of components used by people to access the system of interest (Step 18c) before completing this step.

   After considering the questions, mark an 'X' in each box next to each appropriate response in the "Intermediate Access Points" area on the *Network Access Paths Worksheet* (Vol. 5-8). You are presented with the following options:
   - internal networks
   - external networks
   - others

   If you select "others," be sure to list specific classes of components.
2. When you select a key class of components, document any relevant subclasses or cite specific examples when appropriate. For example, if you select "internal networks," you might find it necessary to further refine the designation if your organization maintains multiple networks. Thus, you could determine that you need to account for two subclasses of internal networks: network A and network B.

(continued on next page)

Activity S3.1: Examine Access Paths (cont.) Phase 2, Process S3, Steps 17-18

Activity Worksheets	*Reference Worksheets*
• Network Access Paths in appropriate Critical Asset Workbook (Vol. 5-8)	• Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 18c

1. Examine which components *people use* to access the system of interest. Consider the following question:
   - From which types of components can people (e.g., users, attackers) access the system of interest?

   As you review how people can access the system of interest, think about access points both internal and external to your organization's networks.

   After considering the question, mark an 'X' in each box next to each appropriate response in the "System Access by People" column area on the *Network Access Paths Worksheet* (Vol. 5-8). You are presented with the following options:
   - on-site workstations
   - laptops
   - PDAs/wireless components
   - home/external workstations
   - others

   If you select "others," be sure to list specific classes of components.
2. When you select a key class of components, document any relevant subclasses or cite specific examples when appropriate. For example, if you select "on-site workstations," you might find it necessary to further refine the designation based on classes of users. Thus, if workstations are configured differently based on how they are used, you could determine that "on-site workstations" includes two subclasses of workstations: staff and management.

(continued on next page)

Activity S3.1: Examine Access Paths (cont.)	Phase 2, Process S3, Steps 17-18
Activity Worksheets • Network Access Path in appropriate Critical Asset Workbook (Vol. 5-8)	*Reference Worksheets* • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 18d

1. Determine if any data storage locations are linked to information on the system of interest. Consider the following question:

   - On which classes of components is information from the system of interest stored for backup purposes?

   After considering the questions, mark an 'X' in each box next to each appropriate response in the "Data Storage Locations" area on the *Network Access Paths Worksheet* (Vol. 5-8). You are presented with the following options:

   - storage devices
   - others

   If you select "others," be sure to list specific classes of components.

2. When you select a key class of components, document any relevant subclasses or cite specific examples when appropriate. For example, if you select "storage devices," you might find it necessary to further refine the designation based on where different types of information are backed up. Thus, you could determine that "storage devices" includes two subclasses of workstations: accounting backups and personnel information backups.

Step 18e

Finally, examine other systems and components that access information, services, or applications from the system of interest. Consider the following questions:

- Which other systems access information or applications from the system of interest?
- Which other classes of components can be used to access critical information or applications from the system of interest?

After considering the question, record the names of applicable systems or components in the blanks provided in the "Other Systems and Components" area on the *Network Access Paths Worksheet* (Vol. 5-8). Mark an 'X' in each box next to a filled-in blank.

S3.2 Analyze Technology-Related Processes

Activity S3.2: Analyze Technology-Related Processes	Phase 2, Process S3, Steps 19-21
Activity Worksheets • Infrastructure Review (Vol. 4)	*Reference Worksheets* • Network Access Path in Critical Asset Workbook (Vol. 5-8)

Background/Definitions

The analysis focus shifts during Activity S3.2. During Activity S2.3, you performed analysis activities from an asset perspective when you identified threats to critical assets. Likewise, during Activity S3.1, you performed analysis activities from an asset perspective when you examined access paths in relation to critical assets.

However, during Activity S3.2, rather than performing analysis activities from an asset perspective, you now assume an infrastructure perspective. During this activity, you analyze the technology-related processes used when configuring and maintaining the computing infrastructure.

During Activity S3.2, you compile information for each class of component that you identified during the previous activity. The information for each class includes

- the critical assets that are related to each class
- the party (or parties) responsible for maintaining and securing each class of components
- the extent to which security is considered when configuring and maintaining each class of components (very much, somewhat, not at all, don't know)
- how you determined the extent to which security is considered when configuring and maintaining each class of components (formal techniques, informal means, other)
- any additional information, notes, and issues you want to record for each class

(continued on next page)

Activity S3.2: Analyze Technology-Related Processes (cont.)	Phase 2, Process S3, Steps 19-21
Activity Worksheets • Infrastructure Review (Vol. 4)	*Reference Worksheets* • Network Access Path in Critical Asset Workbook (Vol. 5-8)

Instructions

Step 19a

1. Review the classes of components you identified for each critical asset during Activity S3.1 on that asset's *Network Access Paths Worksheet* (Vol. 5-8). In this step, you simply mark the path to each class you selected in Steps 18a-18e. Consider the following question:

   - Which classes of components are related to one or more critical assets?

   For each class that is related to one or more critical asset, mark that path on the *Infrastructure Review Worksheet* (Vol. 4).

2. Recall that during Steps 18a-18e, you also documented relevant subclasses or cited specific examples for each class when appropriate. For example, when you selected "on-site workstations," you might have found it necessary to further refine the designation based on classes of users. Thus, if workstations are configured differently based on how they are used, you might have determined that "on-site workstations" includes two subclasses of workstations related to a critical asset: staff and management. As you looked at other critical assets, you might have identified additional subclasses.

   Document any relevant subclasses or specific examples for each class, when appropriate, in the space provided on the *Infrastructure Review Worksheet* (Vol. 4). If you have identified no subclasses or examples for a given class, you can record "all" under that class to denote that there are no variations or subclasses for that particular class of components.

Step 19b

1. Now you are going to note which critical assets are related to each class of components. For example, during the previous activity, you might have noted that "on-site workstations" were part of or related to the systems of interest for three critical assets. In this step, you document that information.

   First, you need to transcribe the name of each critical asset to the *Infrastructure Review Worksheet* (Vol. 4). At the top of *Infrastructure Review Worksheet* (under Step 19b) is an area that is numbered from 1 through 5. This is the space where you should record the names of your organization's critical assets. Document the name of each critical asset in the spaces provided.

2. Consider the following question:

   - Which critical assets are related to each class of components?

   Refer to the *Network Access Paths Worksheets* (Vol. 5-8) for each critical asset and review the information recorded under Steps 18a-18e. For each class you marked on the *Infrastructure Review Worksheet* (Vol. 4) during Step 19a, record which critical assets are related to that class by marking an 'X' in the boxes below the applicable asset names. If you identified specific subclasses for a class of component, be sure to denote which subclasses are related to which critical assets.

(continued on next page)

Activity S3.2: Analyze Technology-Related Processes (cont.)	Phase 2, Process S3, Steps 19-21
Activity Worksheets • Infrastructure Review (Vol. 4)	*Reference Worksheets* • Network Access Path in Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 20

Next, identify the party (or parties) responsible for maintaining and securing each class of components. If you identified more than one subclass for any given class of components, you must identify the party (or parties) responsible for maintaining and securing each subclass.

For each class you marked on the *Infrastructure Review Worksheet* (Vol. 4) during Step 19a, consider the following question:

- Who is responsible for maintaining and securing each class of component?

Record the name of the party or parties responsible for maintaining and securing each class (or subclass when applicable) of component on the *Infrastructure Review Worksheet* (Vol. 4).

Step 21

1. Determine how well you believe each class of components is currently being protected. If you identified more than one subclass for any given class of components, you must determine how well you believe each subclass is currently being protected. There could be variations in how subclasses within the same class are protected, especially if a different party is responsible for configuring and maintaining each subclass.

   Consider the following question:

   - To what extent is security considered when configuring and maintaining each class of components?

   Based on your answer to the question, mark an 'X' on the scale at the point that indicates how much security is considered when configuring and maintaining each class of components. The following points are provided on the *Infrastructure Review Worksheet* (Vol. 4) as references on the scale:

   - *Very much* – You have a considerable amount of objective data related to your estimate. Any reasonable person reviewing the objective data would reach the same conclusion.
   - *Somewhat* – You have a limited amount of objective data related to your estimate. A reasonable person would need to make key inferences and assumptions to reach the same conclusion. However it is likely that a reasonable person would arrive at the same conclusion.
   - *Not at all* – You have little or no objective data related to your estimate. A reasonable person could arrive at a different conclusion because there are little or no objective data upon which to base the estimate.
   - *Don't Know* – You do not have enough experience and expertise to make a plausible guess.

(continued on next page)

Activity S3.2: Analyze Technology-Related Processes (cont.)	Phase 2, Process S3, Steps 19-21
Activity Worksheets • Infrastructure Review (Vol. 4)	*Reference Worksheets* • Network Access Path in Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 21(cont.)

2. You should also specifically note the sources for any data you used when determining the extent to which security is considered when configuring and maintaining each class of components.

   Consider the following question:

   - How do you know?

   Mark an 'X' in the box next to the best response to the above question from the following options on the *Infrastructure Review Worksheet* (Vol. 4):

   - *Formal Techniques* – You employed rigorous data gathering and analysis techniques to reach your conclusion. This can include a targeted vulnerability evaluation of the computing infrastructure by experienced personnel, a formal audit of components by qualified personnel, or any other formal evaluation/analysis technique. Provide any additional information in the "Notes/Issues" column when appropriate.
   - *Informal Means* – You performed a cursory evaluation of the situation to reach your conclusion. This can include a very limited vulnerability evaluation of the computing infrastructure, a limited review or audit of components, or any other incomplete or ad hoc technique. This can also include any rigorous data gathering and analysis techniques performed by inexperienced personnel. Provide any additional information in the "Notes/Issues" column when appropriate.
   - Other – Use this category to identify any other means you used to reach your conclusion that does not fall into either of the above categories. Provide any additional information in the "Notes/Issues" column when appropriate.

   Also document any other relevant notes or issues related to a component class in the space provided on the *Infrastructure Review Worksheet* (Vol. 4) when appropriate.

(continued on next page)

Activity S3.2: Analyze Technology-Related Processes (cont.)	Phase 2, Process S3, Steps 19-21
Activity Worksheets • Infrastructure Review (Vol. 4)	*Reference Worksheets* • Network Access Path in Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Gap Analysis

Refine Phase 1 information based on the analysis of access paths and technology-related processes. Perform the following tasks:

- Update the *Risk Profile Worksheet* (Vol. 5-8) for each critical asset when appropriate. Mark any additional branches of the threat trees if your Phase 2 analysis warrants it (Step 12). Document any additional context for each new branch you mark (Steps 13-16). Also look for instances where you can revise existing areas of concern by adding additional details, or where you can identify new areas of concern (Step 16).
- Update the *Security Practices Worksheet* (Vol. 4) when appropriate. Revise your responses to the survey questions if your Phase 2 analysis warrants it. Also look for instances where you can revise existing security practices and organizational vulnerabilities by adding additional details, or where you can identify new security practices and organizational vulnerabilities. Finally, review the information for each security practice area for which you have made additions or changes, and revise the stoplight status for that area when appropriate.

Action Items, Notes, and Recommendations

1. Document all action items you identified during Process S3 on the *Action List Worksheet* (Vol. 9).

   Include the following information for each action item:

   - a description of the action
   - responsibility for completing the action
   - a date for completing the action
   - any management actions that could help facilitate completion of the action

2. Document notes relevant to the activities in Process S3 on the *Notes and Recommendations Worksheet* (Vol. 9).
3. Document all recommendations from Process S3 that you want to consider during Process S5 on the *Notes and Recommendations Worksheet* (Vol. 9).

Phase 3: Develop Security Strategy and Plans

During Phase 3, the analysis team identifies risks to the organization's critical assets and decides what to do about them. Based on an analysis of the information gathered, the team creates a protection strategy for the organization and mitigation plans to address the risks to the critical assets. The OCTAVE-S worksheets used during Phase 3 are highly structured and tightly linked to the OCTAVE catalog of practices, enabling the team to relate its recommendations for improvement to an accepted benchmark of security practice. Table 3 depicts the processes and activities of Phase 3.

Table 3: Processes and Activities of Phase 3

Phase	Process	Activity
Phase 3: Develop Security Strategy and Plans	Process S4: Identify and Analyze Risks	S4.1 Evaluate Impacts of Threats
		S4.2 Establish Probability Evaluation Criteria
		S4.3 Evaluate Probabilities of Threats
	Process S5: Develop Protection Strategy and Mitigation Plans	S5.1 Describe Current Protection Strategy
		S5.2 Select Mitigation Approaches
		S5.3 Develop Risk Mitigation Plans
		S5.4 Identify Changes to Protection Strategy
		S5.5 Identify Next Steps

Process S4: Identify and Analyze Risks

This process focuses on evaluating the impact and probability of threats to critical assets and establishing probability evaluation criteria.

S4.1 Evaluate Impacts of Threats

Activity S4.1: Evaluate Impacts of Threats Phase 3, Process S4, Step 22

Activity Worksheets	*Reference Worksheets*
• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	• Impact Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Background/Definitions

Risk – the possibility of suffering harm or loss. Risk refers to a situation where a person could do something undesirable or a natural occurrence could cause an undesirable outcome, resulting in a negative impact or consequence.

A risk is composed of

- an event
- uncertainty
- a consequence

In information security, the basic event is a threat.

Uncertainty is embodied in much of the information gathered during the OCTAVE-S evaluation. There is uncertainty surrounding whether a threat will occur and whether the organization is sufficiently protected against the threat actor. Uncertainty is often represented using likelihood of occurrence, or probability.

The consequence that ultimately matters in information security risk is the resulting impact on the organization due to a threat. Impact describes how an organization might be affected based on the following threat outcomes:

- disclosure of a critical asset
- modification of a critical asset
- loss/destruction of a critical asset
- interruption of a critical asset

The outcomes listed above are directly related to assets; they describe the effect of threats on assets. Impact is focused on the organization; it is the direct link back to the organization's mission and business objectives.

In Activity S1.1, impact evaluation criteria were created for the following impact areas:

- reputation/customer confidence
- life/health of customers
- fines/legal penalties
- financial
- productivity
- other

(continued on next page)

Activity S4.1: Evaluate Impacts of Threats (cont.) Phase 3, Process S4, Step 22

Activity Worksheets	*Reference Worksheets*
• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	• Impact Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions

Note: Before you begin Process S4, review any notes and recommendations you recorded on the *Notes and Recommendations Worksheet* (Vol. 9) during previous processes. These notes and recommendations could be relevant to the activities you will conduct during Process S4.

Step 22

Note: Before evaluating potential impacts on the organization resulting from threats to critical assets, you should review critical asset and threat information that you documented previously during the evaluation.

1. Review the threat information you recorded on the *Risk Profile Worksheet* (Vol. 5-8) for each critical asset. Focus on the following items:
   - threats to the critical assets
   - threat context (threat actors, motive, history)
   - additional threat context
2. Review the information you recorded on each *Critical Asset Worksheet* (Vol. 5-8). Focus on the following items:
   - rationale for selecting related assets
   - security requirements
   - most important security requirement
3. Review the information you recorded on the *Impact Evaluation Criteria Worksheet* (Vol. 4). Focus on how you defined high, medium, and low impacts for your organization.

   Use the impact evaluation criteria to evaluate each threat's impact on your organization's mission and business objectives. Be sure to review the criteria you recorded for the following areas:
   - reputation/customer confidence
   - life/health of customers
   - fines/legal penalties
   - financial
   - productivity
   - other

(continued on next page)

Activity S4.1: Evaluate Impacts of Threats (cont.)	Phase 3, Process S4, Step 22
Activity Worksheets • Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	*Reference Worksheets* • Impact Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 22 (cont.)

4. For each critical asset, consider the following questions for each threat to that asset:
   - What is the potential impact to the organization's reputation?
   - What is the potential impact on customer confidence?
   - What is the potential impact to customers' health or safety?
   - What is the potential impact to staff members' health or safety?
   - What fines or legal penalties could be imposed on the organization?
   - What is the potential financial impact to the organization?
   - What is the potential impact to the organization's or customers' productivity?
   - What other impacts could occur?

   As you review the questions, think about the potential impact on your organization due to each active threat.

   Note: Each of the above questions is linked to an impact area.

5. After reviewing the above questions, compare the potential impacts you discussed for each impact area against the impact evaluation criteria for that area.

   Using the impact evaluation criteria as a guide, assign an impact measure (high, medium, or low) for each active threat.

   Document each impact on the *Risk Profile Worksheet* (Vol. 5-8) by recording
   - "H" for each high impact
   - "M" for each medium impact
   - "L" for each low impact

   Note: You might identify multiple impacts for a given threat, which could lead to more than one impact value for a given impact area. If this happens, record the highest value for that impact area on the *Risk Profile Worksheet* (Vol. 5-8).

S4.2 Establish Probability Evaluation Criteria

Activity S4.2: Establish Probability Evaluation Criteria	Phase 3, Process S4, Step 23
Activity Worksheets • Probability Evaluation Criteria (Vol. 4)	*Reference Worksheets* • Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)

Background/Definitions

Probability – the likelihood that an event will occur

Probability value – a qualitative measure of a threat's probability (high, medium, or low)

Probability evaluation criteria – a set of qualitative measures used to estimate the likelihood of a threat's occurrence. Probability evaluation criteria define frequency ranges for high, medium, and low probabilities; they indicate how often threats occur over a common period of time.

Time between events – an estimate of how frequently an event might occur (e.g., weekly, once every two years)

Annualized frequency – the projected likelihood of a threat's occurrence in a given year

Information security threat probabilities are estimated using a combination of objective data, subjective experience, and expertise. If you are using OCTAVE-S for the first time, you likely lack objective data related to threats. You also might lack experience and expertise in information security and/or risk management. ***For this reason, probability is considered to be optional in OCTAVE-S.*** Each team needs to decide whether to use probability as well as how to use it.

In OCTAVE-S, probability values are defined by a set of evaluation criteria that are categorized according to frequency of occurrence. Probability evaluation criteria define a standard set of definitions for probability values. These criteria define high, medium, and low measures of threat probabilities.

Probability measures are defined by considering a range of frequencies (i.e., the likelihood of a threat's occurrence in a given year):

- daily
- weekly
- monthly
- 4 times per year
- 2 times per year
- once per year
- once every 2 years
- once every 5 years
- once every 10 years
- once every 20 years
- once every 50 years

(continued on next page)

Activity S4.2: Establish Probability Evaluation Criteria (cont.)	Phase 3, Process S4, Step 23
Activity Worksheets • Probability Evaluation Criteria (Vol. 4)	*Reference Worksheets* • Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 23 (optional)

1. Your goal is to define probability measures based on how often threats are likely to occur.

   Review the following information from the *Risk Profile Worksheet* (Vol. 5-8):

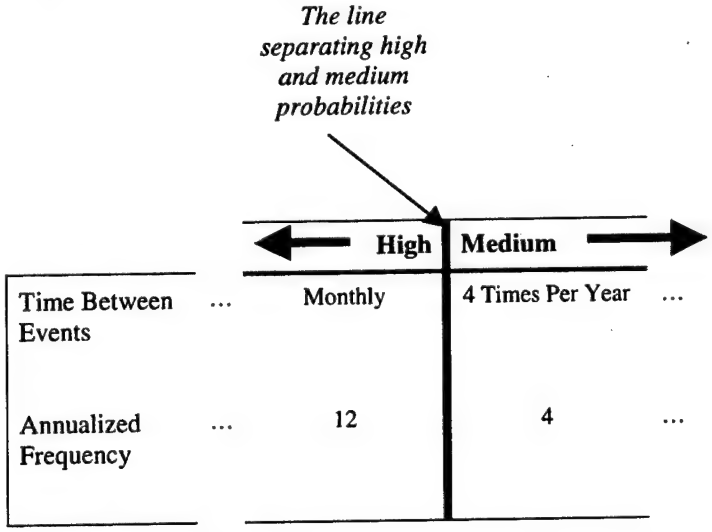
   - the types of threats to critical assets
   - how often each threat has occurred in the past (history)
   - any additional relevant information you recorded

2. Consider the following questions:

   - What defines a "high" likelihood of occurrence? How often must a threat occur to be considered a high-probability threat?
   - What defines a "medium" likelihood of occurrence? How often must a threat occur to be considered a medium-probability threat?
   - What defines a "low" likelihood of occurrence? How often must a threat occur to be considered a low-probability threat?

3. On the *Probability Evaluation Criteria Worksheet* (Vol. 4), draw vertical lines that separate high from medium probabilities and medium from low probabilities.

   Be sure to synchronize the boundaries between levels of probability. For example, when drawing the distinction between high and medium probabilities, you might draw a vertical line between monthly events and events that occur four times a year. This is illustrated in the diagram below.



(continued on next page)

Activity S4.2: Establish Probability Evaluation Criteria (cont.) Phase 3, Process S4, Step 23

Activity Worksheets	*Reference Worksheets*
• Probability Evaluation Criteria (Vol. 4)	• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 23 (cont.)

What if an event occurs six times a year? Should that threat be assigned a high or medium probability? You need to make sure that your criteria have no such gaps. In this case, you could

A. Change the boundary for medium probability threats to "less than monthly" (i.e., <12). This is shown below.

The boundary for medium probabilities has been changed

		High	Medium	
Time Between Events	...	Monthly	~~4 Times Per Year~~ *Less Than Monthly*	...
Annualized Frequency	...	12	4 *<12*	...

B. Change the boundary for high-probability threats to "greater than four times a year" (i.e., >4).

The boundary for high probabilities has been changed

		High	Medium	
Time Between Events	...	~~Monthly~~ *Greater Than 4 Times Per Year*	4 Times Per Year	...
Annualized Frequency	...	~~12~~ *>4*	4	...

(continued on next page)

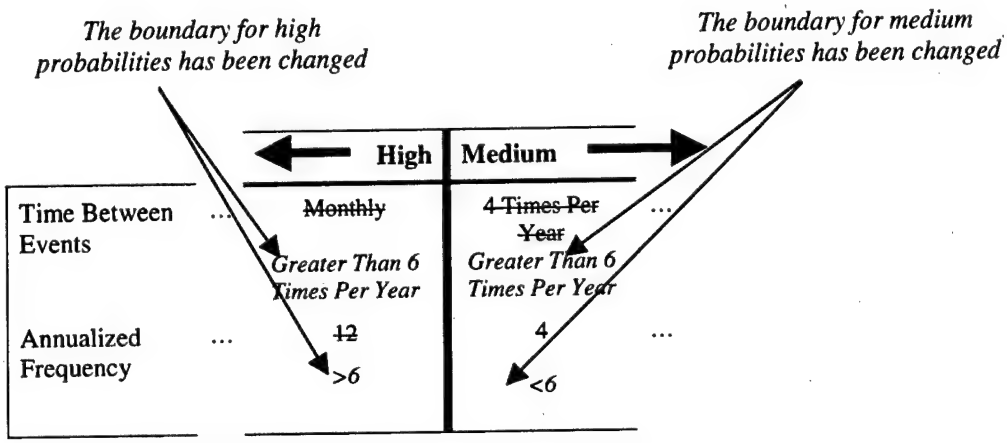
Activity S4.2: Establish Probability Evaluation Criteria (cont.) Phase 3, Process S4, Step 23

Activity Worksheets	*Reference Worksheets*
• Probability Evaluation Criteria (Vol. 4)	• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 23 (cont.)

C. Change the boundaries for both high- and medium-probability threats. The boundary for high-probability threats could be changed to "six times a year," while the boundary for medium-probability threats could be "less than six times a year." This is shown below.



The key is to ensure that there are no gaps between your definitions of "high" and "medium" measures of probability and between your definitions of "medium" and "low" measures of probability.

S4.3 Evaluate Probabilities of Threats

Activity S4.3: Evaluate Probabilities of Threats	Phase 3, Process S4, Step 24
Activity Worksheets • Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	*Reference Worksheets* • Probability Evaluation Criteria (Vol. 4)

Background/Definitions

A risk is composed of

- an event
- uncertainty
- a consequence

Uncertainty is embodied in much of the information gathered during the evaluation. There is uncertainty surrounding whether a threat will occur and whether the organization is sufficiently protected against the threat actor. Uncertainty is often represented using likelihood of occurrence, or probability.

In Activity S4.2, probability evaluation criteria were created for high, medium, and low threat probabilities.

Instructions

Step 24 (optional)

1. The table below highlights information for each active threat that you may have recorded on each critical asset's *Risk Profile Worksheet* (Vol. 5-8).

Type of Information	Step Number
Contextual information about threat actors	Step 13
The motive for deliberate actions by human actors	Step 14
The history of each active threat	Step 15
Areas of concern	Step 16

For each active threat, review any information you recorded for that threat.

Note: When you estimate probability, you will use a threat's history as a basis.

Consider the following question for each threat:

- How likely is the threat to occur in the future?

Review the history of the threat and assign that threat a qualitative probability value (high, medium, or low) based on the probability evaluation criteria that you created in Activity S4.2 (Step 23) and the history of that threat. Probability evaluation criteria are documented on the *Probability Evaluation Criteria Worksheet* (Vol. 4).

Note: Do **not** record probability values on the *Risk Profile Worksheet* (Vol. 5-8) at this time. You should not record probabilities until later in Step 24.

(continued on next page)

Activity S4.3: Evaluate Probabilities of Threats (cont.)	Phase 3, Process S4, Step 24
Activity Worksheets • Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	*Reference Worksheets* • Probability Evaluation Criteria (Vol. 4)

Instructions (cont.)

Step 24 (cont.)

2. Consider the following question for each threat:
   - Does any of the other information you recorded for the threat change the estimate based on history?

   Consider the following information you recoded on the *Risk Profile Worksheets* (Vol. 5-8):
   - motive for deliberate actions by human actors
   - summary of computing infrastructure vulnerabilities for network threats and malicious code (if it has been estimated)
   - summary of physical infrastructure vulnerabilities for physical threats (if it has been estimated)
   - contextual information about threat actors
   - specific examples of threats
3. Adjust your estimate of any threat probability if you believe that the information warrants it. Refer to the probability criteria when adjusting probability estimates.

   Document each probability on the *Risk Profile Worksheet* (Vol. 5-8) by recording
   - "H" for each high probability
   - "M" for each medium probability
   - "L" for each low probability

   Note: Because each branch on the threat tree represents multiple specific threats, you might identify multiple probabilities for a given threat; which could lead to more than one probability value for a given branch. If this happens, record the highest value for that impact area on the *Risk Profile Worksheet* (Vol. 5-8).

(continued on next page)

Activity S4.3: Evaluate Probabilities of Threats (cont.)	Phase 3, Process S4, Step 24
Activity Worksheets • Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	*Reference Worksheets* • Probability Evaluation Criteria (Vol. 4)

Instructions (cont.)

Step 24 (cont.)

4. Consider the following question for each threat:
   - How confident are you in your estimate of probability for this threat?

   Consider the following:
   - accuracy of history data
   - confidence in your estimate of motive strength (where applicable)
   - comprehensiveness of the evaluation of the computing infrastructure vulnerabilities (where applicable)
   - comprehensiveness of the evaluation of the physical infrastructure vulnerabilities (where applicable)

   Next to each threat probability value on the *Risk Profile Worksheet* (Vol. 5-8) is a scale for confidence with the following defined points: very much, somewhat, and not at all. Based on your answer to the above question, mark an 'X' on the scale at the point that indicates your confidence in the probability value for that threat. The following points are provided as references on the scale:
   - *Very* – You have a considerable amount of objective data related to your estimate. Any reasonable person reviewing the objective data would reach the same conclusion.
   - *Somewhat* – You have a limited amount of objective data related to your estimate. A reasonable person would need to make key inferences and assumptions to reach the same conclusion. However it is likely that a reasonable person would arrive at the same conclusion.
   - *Not at all* – You have little or no objective data related to your estimate. A reasonable person could arrive at a different conclusion because there are little or no objective data upon which to base the estimate.

(continued on next page)

Activity S4.3: Evaluate Probabilities of Threats (cont.) Phase 3, Process S4, Step 24

Activity Worksheets	*Reference Worksheets*
• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	• Probability Evaluation Criteria (Vol. 4)

Instructions (cont.)

Action Items, Notes, and Recommendations

1. Document all action items that you identified during Process S4 on the *Action List Worksheet* (Vol. 9).

   Remember to include the following information for each action item:

   - a description of the action
   - responsibility for completing the action
   - a date for completing the action
   - any management actions that could help facilitate completion of the action

2. Document notes relevant to the activities in Process S4 on the *Notes and Recommendations Worksheet* (Vol. 9).
3. Document all recommendations from Process S4 that you want to consider during Process S5 on the *Notes and Recommendations Worksheet* (Vol. 9).

Process S5: Develop Protection Strategy and Mitigation Plans

This process focuses on defining a protection strategy and mitigation plans as well as the next steps needed to implement the results of the OCTAVE-S evaluation.

S5.1 Describe Current Protection Strategy

Activity S5.1: Describe Current Protection Strategy	Phase 3, Process S5, Step 25
Activity Worksheets • Protection Strategy (Vol. 9)	*Reference Worksheets* • Security Practices (Vol. 4)

Background/Definitions

Protection Strategy – defines the overall strategy employed by an organization to enable, initiate, implement, and maintain its internal security. It is structured according to the security practice areas.

Characteristic – a quality or attribute of a security practice area. Each security practice area comprises multiple characteristics.

Approach – the way in which an organization addresses a characteristic of a security practice area

Task – an activity that must be completed as part of an operational security practice area

Security Practice Areas – groups of practices that are either strategic or operational. Strategic security practice areas are typically broad and tend to affect all risks to all critical assets equally (e.g., documenting a set of security policies for the organization). Operational security practice areas focus on day-to-day tasks and can be targeted toward mitigating specific risks to specific assets (e.g., checking a specific system for default accounts).

A protection strategy defines how an organization intends to raise or maintain the existing level of security. Its objective is to provide a direction for future information security efforts rather than to find an immediate solution to every security vulnerability and concern.

Since a protection strategy provides organizational direction with respect to information security activities, it is structured according to security practice areas. The security practice areas are illustrated in the table below.

Strategic Practice Areas	Operational Practice Areas
1. Security Awareness and Training	7. Physical Access Control
2. Security Strategy	8. Monitoring and Auditing Physical Security
3. Security Management	9. System and Network Management
4. Security Policies and Regulations	10. Monitoring and Auditing IT Security
5. Collaborative Security Management	11. Authentication and Authorization
6. Contingency Planning/Disaster Recovery	12. Vulnerability Management
	13. Encryption
	14. Security Architecture and Design
	15. Incident Management

(continued on next page)

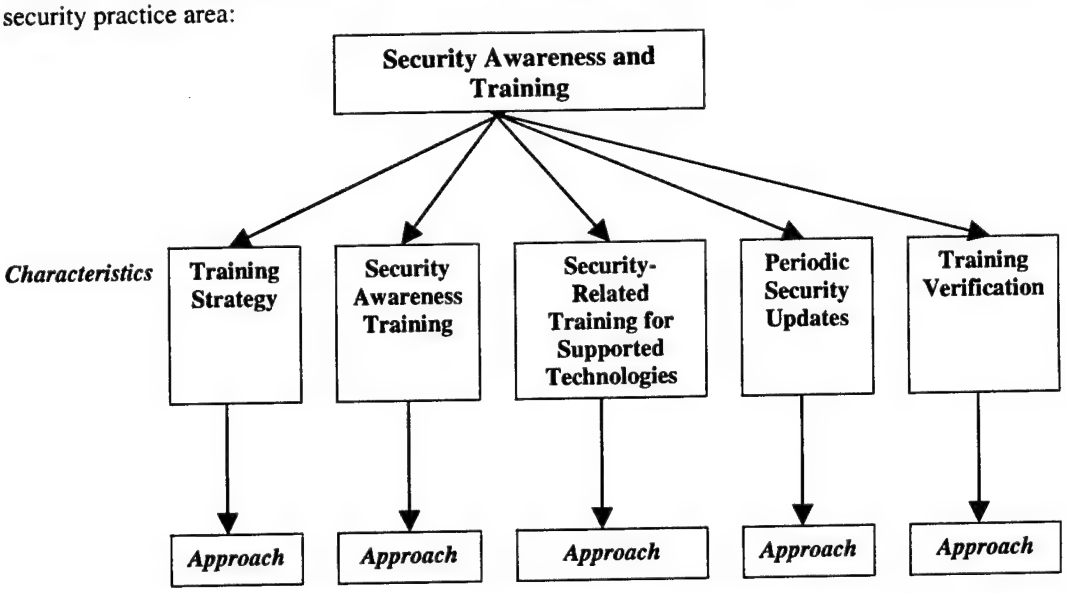
Activity S5.1: Describe Current Protection Strategy (cont.) Phase 3, Process S5, Step 25

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Background/Definitions (cont.)

In OCTAVE-S, each security practice area has multiple characteristics that must be addressed. The type of characteristics is different for strategic and operational security practice areas.

The following diagram depicts the characteristics for *Security Awareness and Training*, a strategic security practice area:



Each *strategic* security practice area has a unique set of characteristics. Refer to the *Protection Strategy Worksheet* (Vol. 9) to see the characteristics for the strategic security practice areas. The *Protection Strategy Worksheet* (Vol. 9) provides a range of approaches for each characteristic. Each characteristic will have a unique approach. For example, the range of approaches for *Training Verification* includes

- ❑ The organization has formal mechanisms for tracking and verifying that staff members receive appropriate security-related training.
- ❑ The organization has informal mechanisms for tracking and verifying that staff members receive appropriate security-related training.
- ❑ The organization has no mechanisms for tracking and verifying that staff members receive appropriate security-related training.
- ❑ _____

The blank is provided for any unique approaches implemented by an organization.

Note: Only one approach is selected for each characteristic of a strategic security practice area.

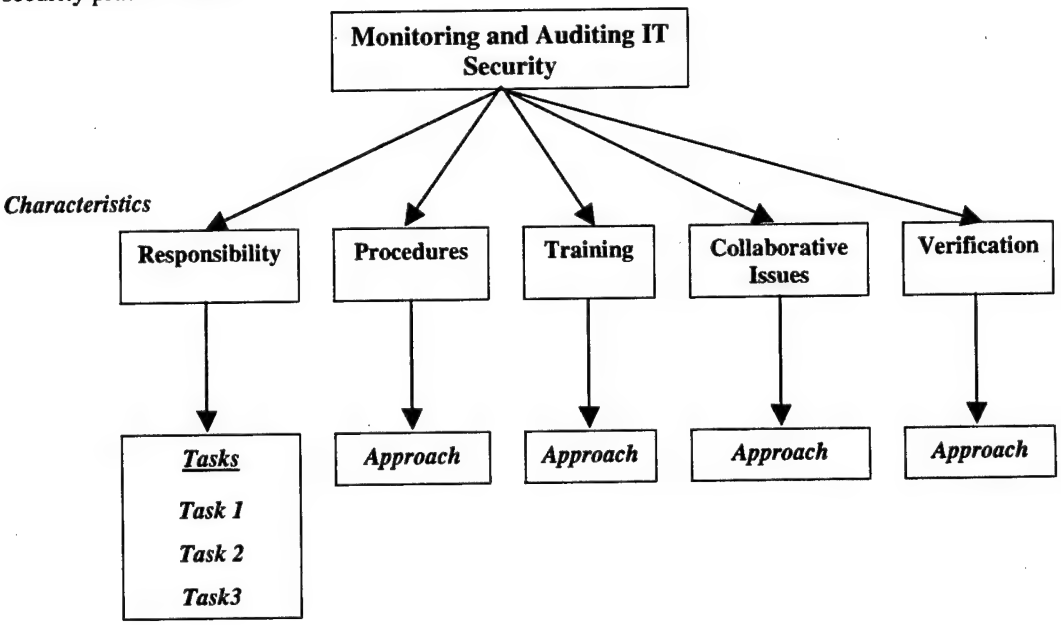
(continued on next page)

Activity S5.1: Describe Current Protection Strategy (cont.) Phase 3, Process S5, Step 25

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Background/Definitions (cont.)

The following diagram depicts the strategy for *Monitoring and Auditing IT Security*, an operational security practice area:



All *operational* security practice areas have identical characteristics (as illustrated above) with one exception. The *Encryption* security practice area breaks the *Training* characteristic into the following two characteristics: *Information Technology Training* and *Staff Training*. This is the only such exception for the operational security practice areas.

The *Responsibility* characteristic defines who has accountability for each task of an operational security practice area. Responsibility for a task can be assigned to people in your organization, to third parties, or to a combination of people in your organization and third parties.

If people from your organization have responsibility for some or all tasks of an operational security practice area, you need to assign an approach to the *Procedures* and *Training* characteristics.

If people from a third party have responsibility for some or all tasks of an operational security practice area, you need to assign an approach to the *Collaborative Issues* and *Verification* characteristics.

(continued on next page)

Activity S5.1: Describe Current Protection Strategy (cont.) Phase 3, Process S5, Step 25

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Background/Definitions (cont.)

Refer to the *Protection Strategy Worksheet* (Vol. 9) to see the characteristics for all operational security practice areas. The *Protection Strategy Worksheet* (Vol. 9) provides a range of tasks for the *Responsibility* characteristic and a range of approaches for the other characteristics.

For example, the range of tasks for the *Responsibility* characteristic of *Monitoring and Auditing IT Security* includes

- ❑ using system and network monitoring tools to track system and network activity
- ❑ auditing the firewall and other security components periodically for compliance with policy
- ❑ investigating and addressing any unusual activity that is identified
- ❑ _____

The blank is provided for any unique tasks required by an organization.

Note: You typically select multiple tasks for the *Responsibility* characteristic. However, for each of the remaining characteristics of an operational security practice area, only one approach is selected.

The range of approaches for the *Procedures* characteristic of *Monitoring and Auditing IT Security* includes

- ❑ The organization has formally documented procedures for monitoring network-based access to systems and networks.
- ❑ The organization has some formally documented procedures for monitoring network-based access to systems and networks. Some procedures in this area are informal and undocumented.
- ❑ The organization has informal and undocumented procedures for monitoring network-based access to systems and networks.
- ❑ _____

The blank is provided for any unique approaches implemented by an organization.

Note: The protection strategy and the security practices survey examine two different facets of security practice areas. The protection strategy describes the processes used to perform activities in each security practice area. The extent to which processes are formally defined is explored. The stoplight status on the security practices survey indicates how well the analysis team believes its organization is performing in each area. An organization could be performing very well in an area, but have very informal processes. Likewise, an organization could have significant room for improvement despite having very formal policies and procedures.

(continued on next page)

Activity S5.1: Describe Current Protection Strategy (cont.)	Phase 3, Process S5, Step 25
Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Instructions

Note: Before you begin Process S5, review any notes and recommendations you recorded on the *Notes and Recommendations Worksheet* (Vol. 9) during previous processes. These notes and recommendations could be relevant to the activities you will conduct during Process S5.

Also review all action items you recorded on the *Action List Worksheet* (Vol. 9) during previous processes. These action items could be relevant to the activities you will conduct during Process S5.

Step 25

Note: The characteristics for a strategic security practice area are different than those for an operational security practice area. The instructions examine how to address each type of security practice area separately.

1. Review the information contained on the *Security Practices Worksheet* (Vol. 4). Pay attention to the following information for each security practice area:
   - the stoplight status
   - the extent to which each security practice for an area is reflected in the organization
   - what the organization is currently doing well in an area
   - what the organization is not currently doing well in an area
2. Transfer the stoplight status for each security practice area (for both strategic *and* operational security practice areas) from the *Security Practices Worksheet* (Vol. 4) to the designated area on the *Protection Strategy Worksheet* (Vol. 9) before defining the strategy for that area.
3. Develop the protection strategy for each strategic security practice area. The following list includes all strategic security practice areas:

   Strategic Practice Areas

   1. Security Awareness and Training
   2. Security Strategy
   3. Security Management
   4. Security Policies and Regulations
   5. Collaborative Security Management
   6. Contingency Planning/Disaster Recovery

(continued on next page)

Activity S5.1: Describe Current Protection Strategy (cont.) Phase 3, Process S5, Step 25

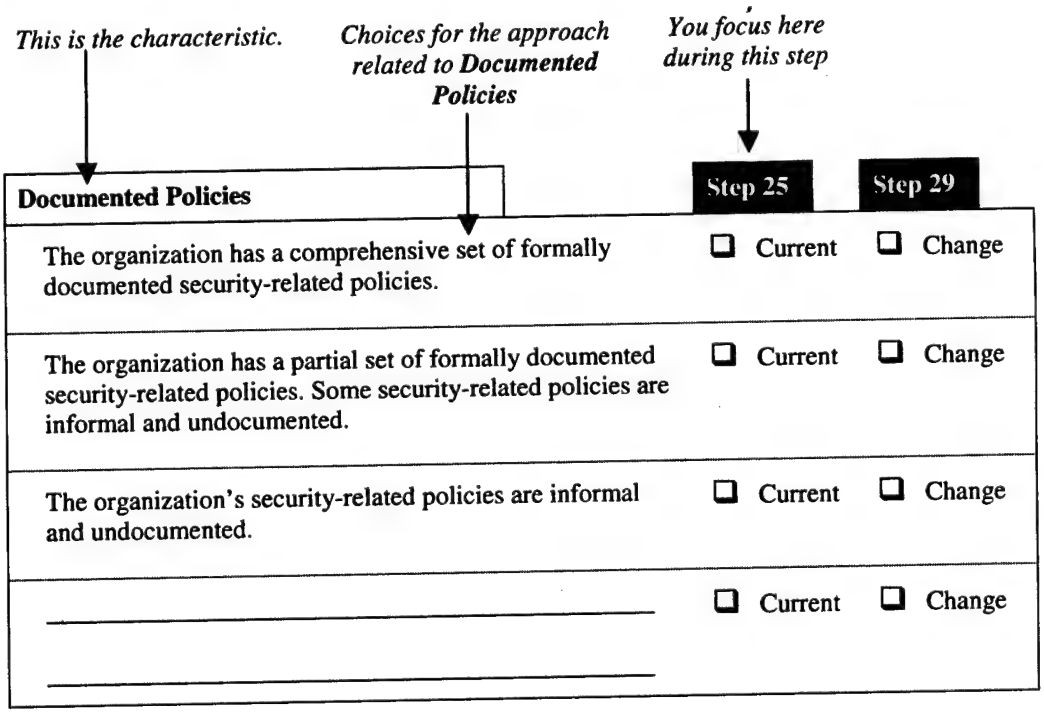
Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Instructions (cont.)

Step 25 (cont.)

4. Each strategic security practice area comprises several unique characteristics. For example, *Security Policies and Regulations* breaks down into the following characteristics:
   - Documented Policies
   - Policy Management
   - Policy Enforcement
   - Staff Awareness
   - Policy and Regulatory Compliance
   - Other

   The following diagram illustrates the *Documented Policies* characteristic for *Security Policies and Regulations*. Review the format of each strategic security practice area on the *Protection Strategy Worksheet* (Vol. 9).



(continued on next page)

Activity S5.1: Describe Current Protection Strategy (cont.)	Phase 3, Process S5, Step 25
Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Instructions (cont.)

Step 25 (cont.)

5. For each characteristic in a given strategic security practice area, consider the following question:

   - What is your organization's approach for addressing this characteristic?

   The *Protection Strategy Worksheet* (Vol. 9) provides several potential answers to the question for each characteristic. If one of the options matches the current situation in your organization, mark an 'X' in the box entitled "Current" next to that option.

   Make sure that you fill in any blanks provided for the option you select. You can change the words provided or add additional words as necessary.

   Note: You are provided with blank lines at the end of each characteristic. If you have a unique answer for how your organization addresses that characteristic, record the approach in the blanks provided and mark an 'X' in the box entitled "Current" next to the blanks.

   You are also provided a blank characteristic for each *strategic* security practice area. If you have a unique characteristic for an area, record your organization's approach in that characteristic and mark an 'X' in the box entitled "Current" next to the approach.

   Do **not** mark an 'X' in the box entitled "Change" at this time. You will consider changes to your organization's protection strategy in Step 32.

   Complete the *Protection Strategy Worksheet* (Vol. 9) for all strategic security practice areas. Make sure that you address all applicable characteristics for each strategic security practice area.

6. Develop the strategy for each operational security practice area. The following list includes all operational security practice areas:

   Operational Practice Areas

   7. Physical Access Control
   8. Monitoring and Auditing Physical Security
   9. System and Network Management
   10. Monitoring and Auditing IT Security
   11. Authentication and Authorization
   12. Vulnerability Management
   13. Encryption
   14. Security Architecture and Design
   15. Incident Management

(continued on next page)

Activity S5.1: Describe Current Protection Strategy (cont.) Phase 3, Process S5, Step 25

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Instructions (cont.)

Step 25 (cont.)

7. Each operational practice area comprises several characteristics. The format for all operational practice areas is fairly consistent. The following table describes each characteristic and when you need to address that characteristic.

Characteristic	Description
Responsibility	This characteristic defines who has responsibility for completing a set of specified tasks for an operational security practice area. The *Responsibility* characteristic includes multiple tasks for which accountability is assigned. This characteristic defines whether accountability for each task rests with people in your organization, with third parties, or with a combination of people in your organization as well as third parties.
Procedures	If people from your organization have responsibility for some or all tasks of an operational security practice area, you must address this characteristic. The *Procedures* characteristic defines the extent to which procedures for an operational security practice area are formally defined.
Training	If people from your organization have responsibility for some or all tasks of an operational security practice area, you must address this characteristic. The *Training* characteristic defines the approach for building staff members' skills in a practice area.
Collaborative Issues	If people from a third party have responsibility for some or all tasks of an operational security practice area, you must address this characteristic. The *Collaborative Issues* characteristic defines the degree to which requirements for an operational security practice area are formally communicated to each third party.
Verification	If people from a third party have responsibility for some or all tasks of an operational security practice area, you must address this characteristic. The *Verification* characteristic defines the degree to which each third party complies with the requirements for an operational security practice area.

Note: If **people in your organization** have sole responsibility for all tasks in an operational security practice area, do **not** complete a strategy for the *Collaborative Issues* and *Verification* characteristics. If **a third party** has sole responsibility for all tasks in an operational security practice area, do **not** complete a strategy for the *Procedures* and *Training* characteristics.

(continued on next page)

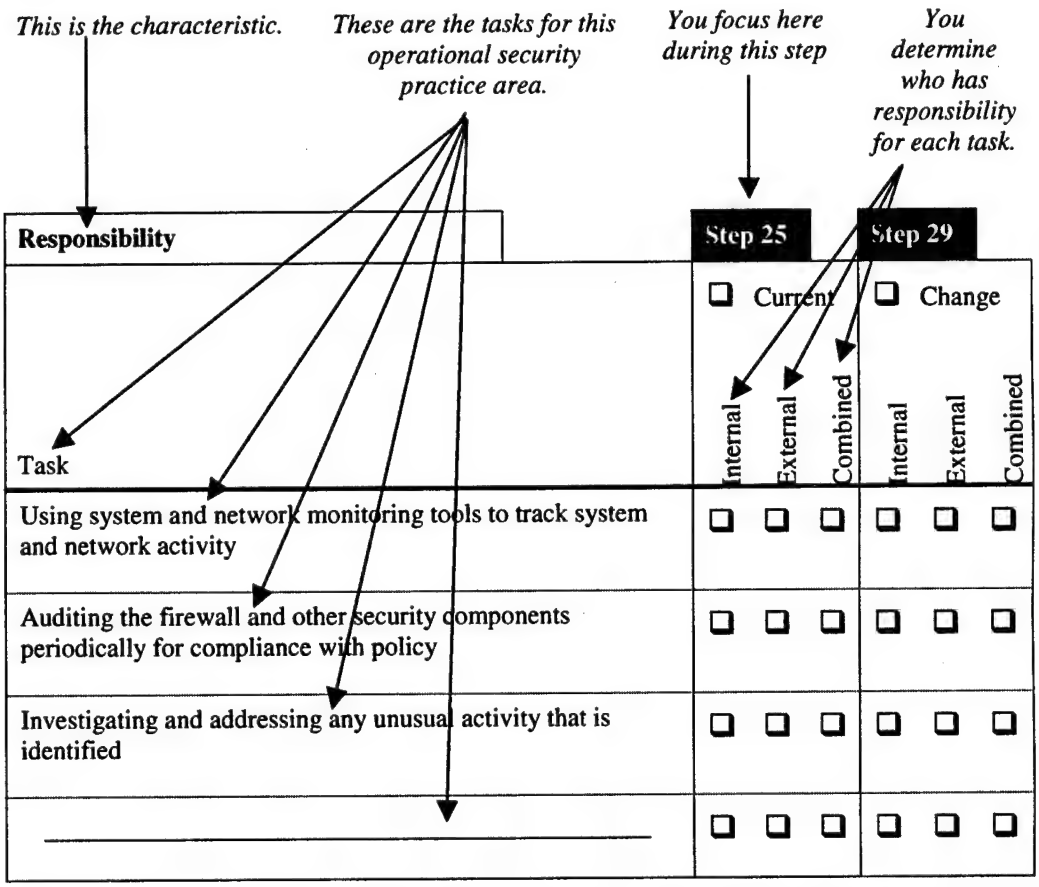
Activity S5.1: Describe Current Protection Strategy (cont.) Phase 3, Process S5, Step 25

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Instructions (cont.)

Step 25 (cont.)

The following diagram illustrates the *Responsibility* characteristic for *Monitoring and Auditing IT Security*.



Review the format of each operational security practice area on the *Protection Strategy Worksheet* (Vol. 9).

Note: The format of the *Responsibility* characteristic was highlighted here because it differs from the format of the other characteristics. The *Responsibility* characteristic for an operational security practice area comprises the tasks that must be performed in that practice area. Each of the other characteristics for an operational security practice area defines the approach for achieving that characteristic. The format of the other characteristics is similar to the format of the characteristics for the strategic security practice areas.

(continued on next page)

Activity S5.1: Describe Current Protection Strategy cont.)	Phase 3, Process S5, Step 25
Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Instructions (cont.)

Step 25 (cont.)

8. The *Protection Strategy Worksheet* (Vol. 9) lists several tasks under the *Responsibility* characteristic for each operational security practice area. Initially you determine who has responsibility for each task for an operational security practice area. First, mark an 'X' in the box entitled "Current."

   For each operational security practice area, consider the following questions:

   - Who is currently responsible for completing each task in this operational security practice area? People in your organization? A third party? A combination of people in your organization and one or more third parties?

   The *Protection Strategy Worksheet* (Vol. 9) lists three options under the current column for each task:

   - Internal – People in your organization are responsible for completing the task.
   - External – One or more third parties are responsible for completing the task.
   - Combined – A combination of people in your organization and one or more third parties are responsible for completing the task.

   Mark an 'X' in the appropriate box for each task. You can change the words provided for a task or add additional words as necessary.

   Note: The *Responsibility* characteristic for each operational security practice area provides several blanks. If you have tasks that are not listed in the protection strategy for an operational security practice area, record those tasks in the blanks provided and mark an 'X' in the appropriate box designating who is responsible for each task.

   Do **not** mark an 'X' in the box entitled "Change" at this time. You will consider changes to your organization's protection strategy in Step 29.

(continued on next page)

Activity S5.1: Describe Current Protection Strategy (cont.)	Phase 3, Process S5, Step 25
Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Instructions (cont.)

Step 25 (cont.)

9. If people from your organization have responsibility for some or all tasks of an operational security practice area, you must designate an approach for the *Procedures* and *Training* characteristics

   Note: The *Encryption* security practice area breaks training into *Information Technology Training* and *Staff Training*. This is the only such exception in the operational security practice areas.

   For the *Procedures* and *Training* characteristics in a given operational security practice area, consider the following question:

   - What is your organization's approach for addressing this characteristic?

   The *Protection Strategy Worksheet* (Vol. 9) provides several potential answers to the question for each characteristic. If one of the options matches the current situation in your organization, mark an 'X' in the box entitled "Current" next to that option.

   Make sure that you fill in any blanks provided for the option you select. You can change the words provided or add additional words as necessary.

   Note: You are provided with blank lines at the end the *Procedures* and *Training* characteristics. If you have a unique approach for how your organization addresses one of those characteristics, record that approach in the blanks provided and mark an 'X' in the box entitled "Current" next to the blanks.

   Do **not** mark an 'X' in the box entitled "Change" at this time. You will consider changes to your organization's protection strategy in Step 29.

(continued on next page)

Activity S5.1: Describe Current Protection Strategy (cont.)	Phase 3, Process S5, Step 25
Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Instructions (cont.)

Step 25 (cont.)

10. If people from a third party have responsibility for some or all tasks of an operational security practice area, you must designate an approach for the *Collaborative Issues* and *Verification* characteristics. Record the name of the third party in the space provided.

    Note: You might have more than one third party providing information security services in an operational security practice area. Complete *Collaborative Issues* and *Verification* characteristics for each third party that provides services in that area.

    For each such characteristic in a given operational security practice area, consider the following question:

    - What is your organization's approach for addressing this characteristic?

    The *Protection Strategy Worksheet* (Vol. 9) provides several potential answers to the question for each characteristic. If one of the options matches the current situation in your organization, mark an 'X' in the box entitled "Current" next to that option.

    Make sure that you fill in any blanks provided for the option you select. You can change the words provided or add additional words as necessary.

    Note: You are provided with blank lines at the end the *Collaborative Issues* and *Verification* characteristics. If you have a unique answer for how your organization addresses one of those characteristics, record the approach in the blanks provided and mark an 'X' in the box entitled "Current" next to the blanks.

    Do **not** mark an 'X' in the box entitled "Change" at this time. You will consider changes to your organization's protection strategy in Step 29.

11. Complete the *Protection Strategy Worksheet* (Vol. 9) for all operational security practice areas. Make sure that you address all applicable characteristics for each operational security practice area.

S5.2 Select Mitigation Approaches

Activity S5.2: Select Mitigation Approaches	Phase 3, Process S5, Steps 26-27
Activity Worksheets • Risk Profile (Vol. 5-8)	*Reference Worksheets* • Impact Evaluation Criteria (Vol. 4) • Probability Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Infrastructure Review (Vol. 4) • Notes and Recommendations (Vol. 9)

Background/Definitions

Mitigation approach – how an organization intends to address a risk. An organization has the following options for each risk: accept, mitigate, or defer.

Accept – a decision made during risk analysis to take no action to address a risk and to accept the consequences should the risk occur. Risks that are accepted typically have a low impact on an organization.

Mitigate – a decision made during risk analysis to address a risk by implementing activities designed to counter the underlying threat. Risks that are mitigated typically have a high impact on an organization.

Defer – a situation where a risk is neither accepted nor mitigated. The impact on the organization due to a deferred risk is above a minimal threshold, but not so large as to be an immediate priority. Deferred risks are watched and reevaluated at some point in the future.

Mitigation area – a security practice area that is designated to be improved in order to mitigate one or more of an organization's security risks

The decision to accept a risk, mitigate it, or defer the decision is based on a number of factors. Impact value is often the primary driver when making the decision. Probability may be used to determine which risks to mitigate first.

Unfortunately, there is no lockstep decision-making process that applies in all circumstances. The risk profile created for each critical asset during OCTAVE-S is a decision support tool. It presents threats, impact values for multiple impact areas, probability values, and the stoplight statuses of the security practice areas, illustrating a picture of the risks affecting that critical asset. An analysis team uses the risk profile to support the mitigation decisions that it makes.

(continued on next page)

Activity S5.2: Select Mitigation Approaches (cont.)	Phase 3, Process S5, Steps 26-27
Activity Worksheets • Risk Profile (Vol. 5-8)	*Reference Worksheets* • Impact Evaluation Criteria (Vol. 4) • Probability Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Infrastructure Review (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions

Step 26

Transfer the stoplight status for each security practice area from the *Security Practices Worksheet* (Vol. 9) to the "Security Practice Areas" section (Step 29) of each critical asset's *Risk Profile Worksheet* (Vol. 5-8).

Note: Some of the security practice areas are "blocked" for each risk. These areas are unlikely to be selected as mitigation areas. Do not record the stoplight status for an area that is "blocked," unless you have determined that it applies to a risk under your current circumstances.

Step 27

Note: There is no single approach for analyzing the information that you recorded throughout the evaluation. One approach is documented in these guidelines. You can select your approach to best suit your analysis team's preferences as well as your organization's accepted practices.

Your ultimate goal in Step 27 is to select three security practice areas as mitigation areas. Based on your organization's security risks as well as funding and staff constraints, you might decide to select fewer or more than three mitigation areas. Use your best judgment.

1. Review the information contained on the following worksheets:
   - *Risk Profile Worksheet* (for each critical asset) (Vol. 5-8)
   - *Critical Asset Worksheet* (for each critical asset) (Vol. 5-8)
   - *Security Practices Worksheet* (Vol. 4)
   - *Infrastructure Review Worksheet* (Vol. 4)

   You might need additional context for interpreting the impact, probability, and vulnerability data on the above worksheets. Review your definitions of impact and probability severity levels on the following worksheets:
   - *Impact Evaluation Criteria Worksheet* (Vol. 4)
   - *Probability Evaluation Criteria Worksheet* (Vol. 4)

(continued on next page)

Activity S5.2: Select Mitigation Approaches (cont.)	Phase 3, Process S5, Steps 26-27
Activity Worksheets • Risk Profile (Vol. 5-8)	*Reference Worksheets* • Impact Evaluation Criteria (Vol. 4) • Probability Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Infrastructure Review (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions (cont.)

Step 27 (cont.)

2. Review all information you recorded throughout the evaluation on the *Notes and Recommendation Worksheets* (Vol. 9). Pay specific attention to any recommendations that you made regarding potential mitigation activities.

   Note: You can review any information that you recorded during the evaluation before you select mitigation approaches. The worksheets highlighted above constitute the minimal set of information you will need during this activity.

3. Consider the following questions:

   - What is driving your selection of mitigation areas?
   - Which impact areas are most important to your organization?
   - How will you factor probability into your decisions?
   - Which security requirement is most important for each critical asset?
   - Which specific areas of concern do you need to address?
   - Which specific security practice areas need the most improvement?
   - Which specific organizational vulnerabilities do you need to address?
   - What other factors will influence your selection of mitigation areas?

   Review risks to your critical assets, keeping the above questions in mind. Start thinking about how to address each risk. You need to start thinking about which risks you intend to mitigate, which you intend to accept, and which you intend to watch and reevaluate at some point in the future.

4. Consider the following question:

   - Which risks need to be mitigated?

   Mark an 'X' in the box entitled "Mitigate" for each risk that you intend to mitigate. Think ahead as you are selecting which risks to mitigate. If you select too many areas, you could be overwhelmed during mitigation planning.

(continued on next page)

Activity S5.2: Select Mitigation Approaches (cont.)	Phase 3, Process S5, Steps 26-27
Activity Worksheets • Risk Profile (Vol. 5-8)	*Reference Worksheets* • Impact Evaluation Criteria (Vol. 4) • Probability Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Infrastructure Review (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions (cont.)

Step 27 (cont.)

5. Consider the following question for all risks that have not yet been assigned a mitigation approach:

   - Which risks are you going to accept?

   Think about the impact on the organization due to each risk. Determine which impacts are low enough that you do not foresee the need to ever take proactive action to prevent them.

   Mark an 'X' in the box entitled "Accept" for these risks in the designated area (Step 27) on the *Risk Profile Worksheet* (Vol. 5-8).

6. For any risks that have still not been assigned a mitigation approach (i.e., those not yet designated as "Mitigate" or "Accept"), consider the following question:

   - Are there any additional risks that you need to mitigate?

   Remember to consider your decision-making drivers as you consider additional areas to select. Mark an 'X' in the box entitled "Mitigate" for each additional risk that you select.

7. To this point, you have selected risks that the organization will mitigate and also identified those risks that the organization will accept. You also likely have some risks that have neither been accepted nor mitigated.

   For those risks that have neither been accepted nor mitigated, you have decided that the potential impacts resulting from these risks were not low enough to accept nor large enough to be designated as a current mitigation priority. Mark an 'X' in the box entitled "Defer" for these risks. Deferred risks are watched and reevaluated at some point in the future.

   You have now assigned a mitigation approach to each risk. Next, you need to select mitigation areas.

(continued on next page)

Activity S5.2: Select Mitigation Approaches (cont.)	Phase 3, Process S5, Steps 26-27
Activity Worksheets • Risk Profile (Vol. 5-8)	*Reference Worksheets* • Impact Evaluation Criteria (Vol. 4) • Probability Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Infrastructure Review (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions (cont.)

Step 27 (cont.)

8. Consider the following questions as you review the risks to all critical assets, also keeping in mind your decision-making drivers:
   - Which security practice areas have the most room for improvement? How would these areas affect the risks that need to be mitigated?
   - Which security practice areas, if selected for mitigation, could mitigate many risks to more than one critical asset?
   - Are there any regulations or policies that need to be considered as you select mitigation areas? If so, which areas would they lead you to select?

   Select three (3) security practice areas as mitigation areas. Be sure to consider any constraints (e.g., funds and staff) when you make your selections. If your situation warrants it, you can select fewer or more than three security practice areas. You must use your best judgment when deciding how many areas to select.

   Note: Once you decide to implement improvements in a security practice area to mitigate your organization's security risks, those practice areas are referred to as mitigation areas.

   For each risk that you have decided to mitigate, circle on the appropriate *Risk Profile Worksheet* (Vol. 5-8) which of the selected security practice areas will mitigate that risk.

(continued on next page)

Activity S5.2: Select Mitigation Approaches (cont.) Phase 3, Process S5, Steps 26-27

Activity Worksheets

- Risk Profile (Vol. 5-8)

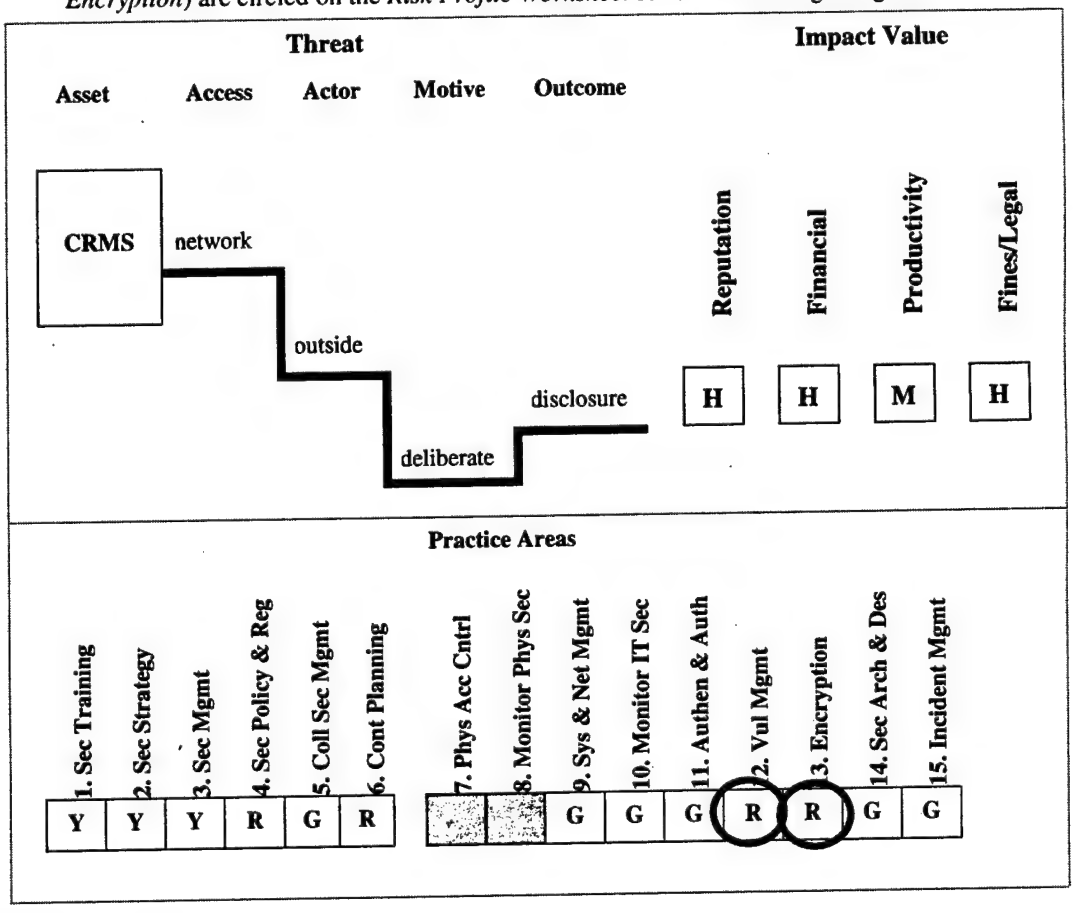
Reference Worksheets

- Impact Evaluation Criteria (Vol. 4)
- Probability Evaluation Criteria (Vol. 4)
- Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)
- Security Practices (Vol. 4)
- Infrastructure Review (Vol. 4)
- Notes and Recommendations (Vol. 9)

Instructions (cont.)

Step 27 (cont.)

The following example illustrates how two mitigation areas (*Vulnerability Management* and *Encryption*) are circled on the *Risk Profile Worksheet* for one risk being mitigated:



(continued on next page)

Activity S5.2: Select Mitigation Approaches (cont.)	Phase 3, Process S5, Steps 26-27
Activity Worksheets • Risk Profile (Vol. 5-8)	*Reference Worksheets* • Impact Evaluation Criteria (Vol. 4) • Probability Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Infrastructure Review (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions (cont.)

Step 27 (cont.)

When you select security practice areas to mitigate your organization's security risks, it is recommended that you also record those areas as well as your rationale for selecting them on the *Notes and Recommendations Worksheet* (Vol. 9).

Remember, there is no single approach for analyzing the information that you recorded throughout the evaluation. Assigning mitigation approaches is not a lockstep process. Different teams will approach the analysis in different ways. Most analysis approaches require considerable discussion and some iteration.

These guidelines present one approach for selecting mitigation approaches and mitigation areas. You can tailor the approach to best suit your analysis team's preferences as well as your organization's accepted practices

S5.3 Develop Risk Mitigation Plans

Activity S5.3: Develop Risk Mitigation Plans	Phase 3, Process S5, Step 28
Activity Worksheets • Mitigation Plan (Vol. 9)	*Reference Worksheets* • Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Protection Strategy (Vol. 9) • Action List (Vol. 9) • Notes and Recommendations (Vol. 9) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

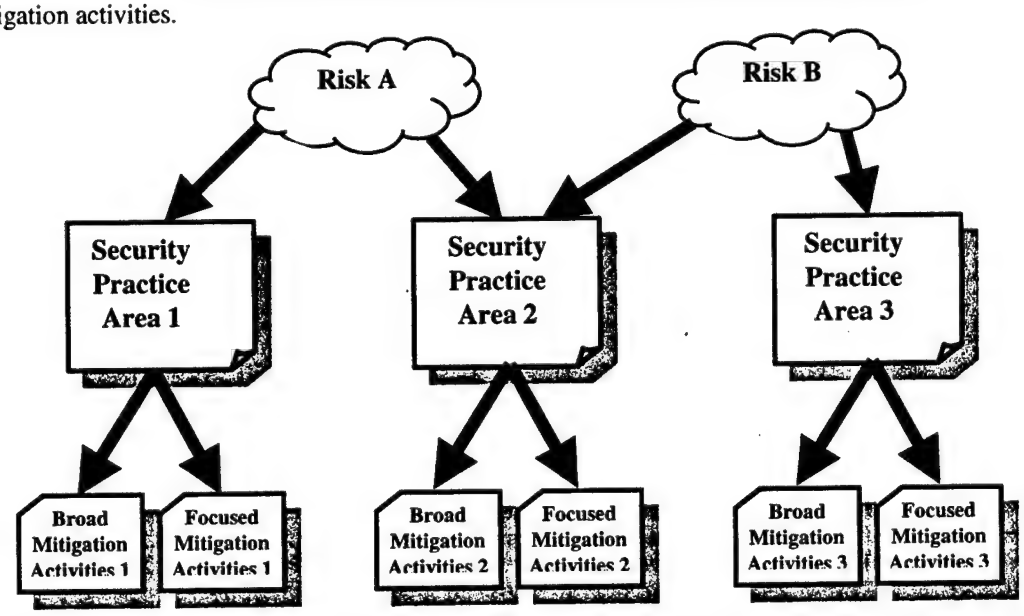
Background/Definitions

Risk mitigation plan – a plan that is intended to reduce the risks to a critical asset. Risk mitigation plans tend to incorporate activities, or countermeasures, designed to counter the threats to the assets.

An analysis team creates a separate mitigation plan for each security practice area it selected as a mitigation area during the previous activity (Activity S5.2).

There are two types of mitigation activities: broad mitigation activities and focused mitigation activities.

The following diagram illustrates the relationships among risks, security practice areas, and mitigation activities.



(continued on next page)

Activity S5.3: Develop Risk Mitigation Plans (cont.)	Phase 3, Process S5, Step 28
Activity Worksheets • Mitigation Plan (Vol. 9)	*Reference Worksheets* • Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Protection Strategy (Vol. 9) • Action List (Vol. 9) • Notes and Recommendations (Vol. 9) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Background/Definitions (cont.)

Broad mitigation activities trigger a change in the approach for a security practice area's characteristic. Focused mitigation activities

- do not require a change to the approach for a security practice area's characteristic
- improve how the current approach for a security practice area's characteristic is implemented

Focused mitigation activities are often directed at specific assets or concentrated on specific improvements.

Risk mitigation plans are often linked to enterprise survivability. They are generally designed to reduce the risks that could prevent an organization from achieving its mission by addressing the underlying threats. A mitigation activity can address threats in one or more of the following ways:

- *Recognize* threats as they occur.
- *Resist* threats to prevent them from occurring.
- *Recover* from threats after they occur.

Risk mitigation plans comprise the following elements:

- *mitigation activity* – defines the activities an analysis team is recommending to implement in a security practice area
- *rationale* – documents the reasons for selecting each mitigation activity. The rationale should document whether the activity is intended to recognize threats, resist them, or recover from them.
- *mitigation responsibility* – identifies who must be involved in implementing each activity
- *additional support* – documents any additional support that will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)

(continued on next page)

Activity S5.3: Develop Risk Mitigation Plans (cont.) Phase 3, Process S5, Step 28

Activity Worksheets	*Reference Worksheets*
• Mitigation Plan (Vol. 9)	• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Protection Strategy (Vol. 9) • Action List (Vol. 9) • Notes and Recommendations (Vol. 9) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions

Step 28

1. Review the information contained on the following worksheets:
   - *Risk Profile Worksheet* (for each critical asset) (Vol. 5-8)
   - *Security Practices Worksheet* (Vol. 4)
   - *Protection Strategy Worksheet* (Vol. 9)
   - *Action List Worksheet* (Vol. 9)
   - *Critical Asset Information Worksheet* (for each critical asset) (Vol. 5-8)

   You might need additional context for interpreting the impact, probability, and vulnerability data on the above worksheets. Review your definitions of impact, probability, and vulnerability severity levels on the following worksheets:
   - *Impact Evaluation Criteria Worksheet* (Vol. 4)
   - *Probability Evaluation Criteria Worksheet* (Vol. 4)
2. Review all information that you recorded throughout the evaluation on the *Notes and Recommendation Worksheets* (Vol. 9). Pay specific attention to any recommendations that you made regarding potential mitigation activities.

   Note: You can review any information that you recorded during the evaluation before you select mitigation approaches. The worksheets highlighted above constitute the minimal set of information you will need during this activity.
3. In this step, you create mitigation plans for each security practice area that you selected during the previous activity. For each area you selected, review the range of candidate mitigation activities in the *Candidate Mitigation Activities Guide* for that area. The guide provides possible mitigation activities, but not an exhaustive list. Do not be limited by the activities listed in the guide.

(continued on next page)

Activity S5.3: Develop Risk Mitigation Plans (cont.) Phase 3, Process S5, Step 28

Activity Worksheets	*Reference Worksheets*
• Mitigation Plan (Vol. 9)	• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Protection Strategy (Vol. 9) • Action List (Vol. 9) • Notes and Recommendations (Vol. 9) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 28 (cont.)

4. Consider the following question for each selected mitigation area:
   - What mitigation activities would reduce the risk(s) that led to the selection of this area?
   - What is the rationale for selecting each activity?
   - Who needs to be involved in implementing each activity? Why?
   - What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?

   Develop a mitigation plan for each area you selected.

   Note: Look for instances where you anticipate that an activity will trigger a change to the protection strategy (i.e., broad mitigation activities). Make sure that you record this information in the "Mitigation Activity" area for that activity.

S5.4 Identify Changes to Protection Strategy

Activity S5.4: Identify Changes to Protection Strategy	Phase 3, Process S5, Step 29
Activity Worksheets • Protection Strategy (Vol. 9)	*Reference Worksheets* • Mitigation Plan (Vol. 9) • Security Practices (Vol. 4) • Notes and Recommendations (Vol. 9)

Background/Definitions

An organization's protection strategy defines the approaches used by an organization to enable, initiate, implement, and maintain its internal security, providing a direction for future information security efforts. The protection strategy is structured according to security practice areas highlighted in the table below.

Strategic Practice Areas	**Operational Practice Areas**
1. Security Awareness and Training	7. Physical Access Control
2. Security Strategy	8. Monitoring and Auditing Physical Security
3. Security Management	9. System and Network Management
4. Security Policies and Regulations	10. Monitoring and Auditing IT Security
5. Collaborative Security Management	11. Authentication and Authorization
6. Contingency Planning/Disaster Recovery	12. Vulnerability Management
	13. Encryption
	14. Security Architecture and Design
	15. Incident Management

During Activity S5.1 of OCTAVE-S, an analysis team defines its organization's current protection strategy. During Activity S5.2, the team selects which security practice areas must be improved to mitigate the organization's highest priority risks. Then, during Activity S5.3, the team develops mitigation plans for each security practice area selected as a mitigation area.

Risk mitigation plans can include two types of activities: broad mitigation activities and focused mitigation activities. Broad mitigation activities typically trigger a change in the organization's protection strategy, while focused activities improve how the current protection strategy is implemented. *Each change to the protection strategy must be documented.* Documenting changes to an organization's protection strategy is the goal of Activity S5.4.

(continued on next page)

Activity S5.4: Identify Changes to Protection Strategy (cont.)	Phase 3, Process S5, Step 29
Activity Worksheets • Protection Strategy (Vol. 9)	*Reference Worksheets* • Mitigation Plan (Vol. 9) • Security Practices (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions

Step 29

1. Review the information contained on the following worksheets:
   - *Mitigation Plan Worksheet* (Review each plan.) (Vol. 9)
   - *Protection Strategy Worksheet* (Review the current strategy.) (Vol. 9)
   - *Security Practices Worksheet* (Vol. 4)
   - *Notes and Recommendations Worksheet* (Vol. 9)

   Note: You can review any information that you recorded during the evaluation before you perform this activity. The worksheets highlighted above constitute the minimal set of information you will need during this activity.

2. The diagrams on the next two pages illustrate the areas of the *Protection Strategy Worksheet* (Vol. 9) on which you will focus during this activity.

   Each security practice area comprises several characteristics. The following diagram illustrates the *Documented Policies* characteristic for *Security Policies and Regulations*. This characteristic is typical of most characteristics on the *Protection Strategy Worksheet* (Vol. 9). The exception is the *Responsibility* characteristic (for operational security practice areas), which is shown after the diagram for *Documented Policies*.

(continued on next page)

Activity S5.4: Identify Changes to Protection Strategy (cont.) Phase 3, Process S5, Step 29

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Mitigation Plan (Vol. 9) • Security Practices (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions (cont.)

Step 29 (cont.)

This is the characteristic. *Choices for the approach related to **Documented Policies*** *You focus here during this step*

Documented Policies	Step 25	Step 29
The organization has a comprehensive set of formally documented security-related policies.	❑ Current	❑ Change
The organization has a partial set of formally documented security-related policies. Some security-related policies are informal and undocumented.	❑ Current	❑ Change
The organization's security-related policies are informal and undocumented.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

(continued on next page)

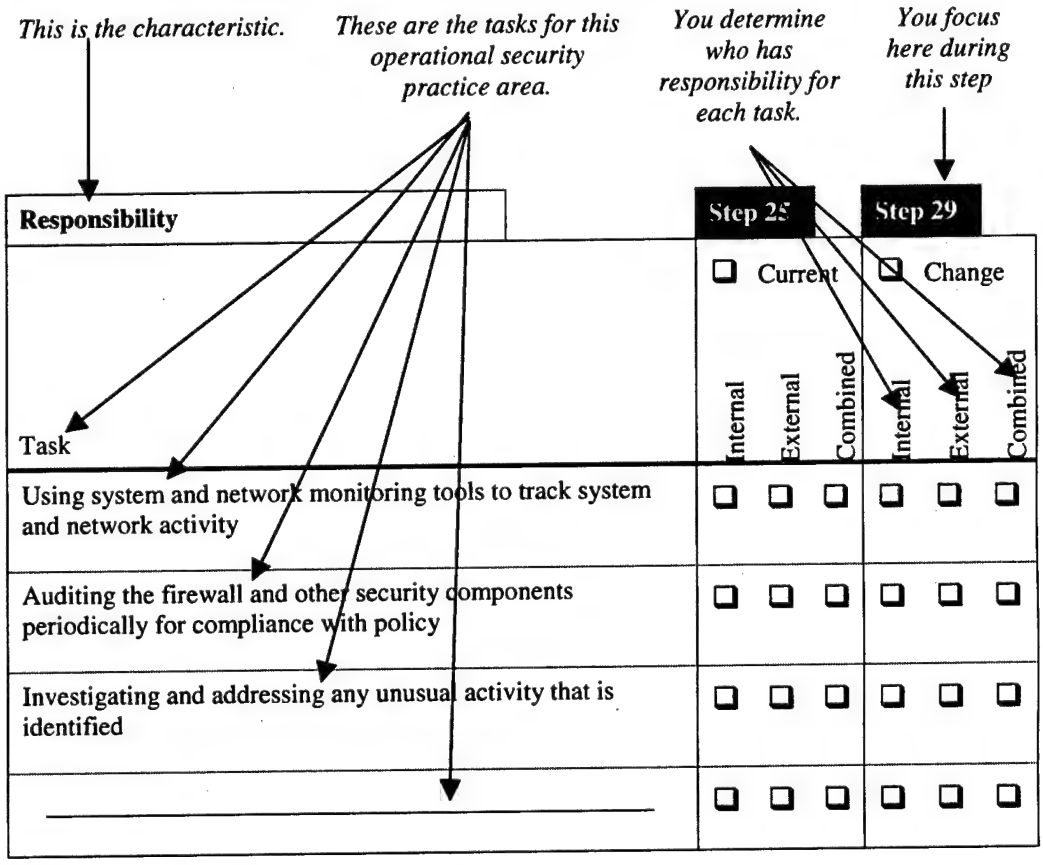
Activity S5.4: Identify Changes to Protection Strategy (cont.) Phase 3, Process S5, Step 29

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Mitigation Plan (Vol. 9) • Security Practices (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions (cont.)

Step 29 (cont.)

The following diagram illustrates the *Responsibility* characteristic for *Monitoring and Auditing IT Security*.



Review the format of the protection strategy for each security practice area.

(continued on next page)

Activity S5.4: Identify Changes to Protection Strategy (cont.)	Phase 3, Process S5, Step 29
Activity Worksheets • Protection Strategy (Vol. 9)	*Reference Worksheets* • Mitigation Plan (Vol. 9) • Security Practices (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions (cont.)

Step 29 (cont.)

3. Consider the following questions for each mitigation activity that you identified during Activity S5.3:
   - Does this mitigation activity indicate a change in the organization's protection strategy?
   - Which characteristic in the security practice area would be affected? How would it be affected?

   If you determine that a mitigation activity affects one of the characteristics in a security practice area, mark an 'X' in the box entitled "Change" next the new approach on the *Protection Strategy Worksheet* (Vol. 9).

   Make sure that you fill in any blanks provided for the option you select. You can change the words provided or add additional words as necessary.

   Note: You are provided with blank lines at the end the all characteristics. If you have a unique answer for your organization's approach for a characteristic, record that strategy in the blanks provided and mark an 'X' in the box entitled "Change" next to the blanks.

4. Review the *Protection Strategy Worksheet* (Vol. 9). Examine the current strategy as well as any changes to the strategy you have identified. Consider the following question as you review the protection strategy:
   - Do you want to make any additional changes to the protection strategy?

   If your answer is yes, then mark those changes on the *Protection Strategy Worksheet* (Vol. 9).

   Next, you need to decide which risks, if any, are driving this change in the protection strategy. Return to the *Risk Profile Worksheet* (Vol. 5-8). Note which risks drove the selection of the new strategy by circling the corresponding security practice area on the appropriate *Risk Profile Worksheet*(s) (Vol. 5-8). (That is, complete Step 26.)

   It is possible that a change in the protection strategy is being driven by factors other than risk (e.g., policy, regulation). If this is the case, you do not need to circle any security practice areas on the *Risk Profile Worksheets* (Vol. 5-8).

   In either case, identify one or more activities that will produce the protection strategy change you identified and document them in the mitigation plan for the appropriate security practice area.

   Note: For any change to the protection strategy that is driven by factors other than risk, be sure to document those factors in the "Rationale" area for that activity.

(continued on next page)

Activity S5.4: Identify Changes to Protection Strategy (cont.)	Phase 3, Process S5, Step 29
Activity Worksheets • Protection Strategy (Vol. 9)	*Reference Worksheets* • Mitigation Plan (Vol. 9) • Security Practices (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions (cont.)

Action Items

Make sure that you document all action items that you identified during Process S6 on the *Action List Worksheet* (Vol. 9).

Remember to include the following information for each action item:

- a description of the action
- responsibility for completing the action
- a date for completing the action
- any management actions that could help facilitate completion of the action

S5.5 Identify Next Steps

Activity S5.5: Identify Next Steps	Phase 3, Process S5, Step 30
Activity Worksheets • Next Steps (Vol. 9)	*Reference Worksheets* • Protection Strategy (Vol. 9) • Mitigation Plan (Vol. 9) • Action List (Vol. 9)

Background/Definitions

Creating a set of next steps marks the end of OCTAVE-S. This activity requires the analysis team to consider what must be done to facilitate implementation of the evaluation's results. Next steps typically address the following four areas:

- management sponsorship for security improvement – defining what management must do to support the implementation of OCTAVE-S results
- monitoring implementation – identifying what the organization will do to track progress and ensure that the results of OCTAVE-S are implemented
- expanding the current information security risk evaluation – determining whether the organization needs to expand the current OCTAVE-S evaluation to include additional critical assets or additional operational areas
- next information security risk evaluation – determining when the organization will conduct its next OCTAVE-S evaluation

Instructions

Step 30

1. Review (at a minimum) the information contained on the following worksheets:
   - *Mitigation Plan Worksheets* (Vol. 9)
   - *Protection Strategy Worksheet* (Vol. 9)
   - *Action List Worksheet* (Vol. 9)

   Consider the following questions:
   - What must management do to support the implementation of OCTAVE-S results?
   - What will the organization do to track progress and ensure that the results of this evaluation are implemented?
   - Will you expand the current OCTAVE-S evaluation to include additional critical assets? Which ones?
   - When will the organization conduct its next OCTAVE-S evaluation?

   Note: The above questions focus on what the senior managers plan to do to enable and encourage implementation of the evaluation results as well as ongoing security improvement activities.

   Determine what steps your organization must take to implement the results of this evaluation. Record those steps on the *Next Steps Worksheet* (Vol. 9).

(continued on next page)

Activity S5.5: Identify Next Steps (cont.)	Phase 3, Process S5, Step 30
Activity Worksheets • Next Steps (Vol. 9)	*Reference Worksheets* • Protection Strategy (Vol. 9) • Mitigation Plan (Vol. 9) • Action List (Vol. 9)

Instructions

Step 30 (cont.)

2. At this point, you have completed an OCTAVE-S evaluation. Make sure that you formally document the results of this evaluation. The format for documenting OCTAVE-S results should fit your organization's normal documentation guidelines and should be tailored to meet your organization's needs.

   Note: It is important to establish a permanent record of evaluation results. The information that you record can serve as source material for subsequent evaluations and is also useful when tracking the status of plans and actions after the evaluation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	January 2005	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
OCTAVE-S Implementation Guide, Version 1.0, Volume 3	F19628-00-C-0003

6. AUTHOR(S)

Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2003-HB-003

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

The Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE®) approach defines a risk-based strategic assessment and planning technique for security. OCTAVE is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organizations (less than 100 people). OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organization's personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization's unique operational security risks. To conduct OCTAVE-S effectively, the team must have broad knowledge of the organization's business and security processes, so it will be able to conduct all activities by itself.

14. SUBJECT TERMS	15. NUMBER OF PAGES
information security, risk management, OCTAVE	94

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL